COMTREND

GS-7624/GS-7620/GS-7424
Gigabit Ethernet Smart-Lite (PoE) Switch
User Manual

GS-7624, 24-Port PoE Gigabit Ethernet Smart-Lite Switch
GS-7620, 20-Port PoE Gigabit Ethernet Smart-Lite Switch
GS-7424, 24-Port Gigabit Ethernet Smart-Lite Switch

Table of Contents

Safety and Regulatory

Audience

This guide is for the networking professional managing the standalone GS-7000 switch series. It is recommended that only professionals with experience working with Comtrend networking devices who are familiar with the Ethernet and local area networking terminology, should service the equipment.

Conventions

The following conventions are used in this manual to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in boldface text.
- Arguments for which you supply values are in italic.
- Square brackets ([ ]) mean optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:

- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

Notes and cautions use the following conventions and symbols:

Note

Means additional information. Notes contain additional useful information or references to material available outside of this document.

Caution

Indicates that the reader must be careful. In a situation where a Caution is listed, a user may cause equipment damage or loss of data.

1. Introduction

Thank you for choosing a Comtrend Ethernet Smart-Lite (PoE)Switch. This device is designed to be operational right out-of-the-box as a standard bridge. In the default configuration, it will forward packets between connecting devices after powered up.

Before you begin installing the switch, make sure you have all of the package contents available, and a PC with a web browser for using web-based system management tools.

1.1. Overview

The Comtrend GS-7620, GS-7624 are Smart-Lite PoE switches with 20 and 24 Gigabit PoE+ ports respectively. The GS-7620 has four combo ports, and the GS-7624 has four SFP slots. The GS-7424 is a Smart-Lite switch with 24 Gigabit ports and four SFP slots. Each model is designed for medium to large network environments. The included standard 19-inch rack-mount brackets allow for integration with any 19-inch mounting system.

1.2. Package contents

Before using the product, check that the items listed below are included and in good condition. If any item does not accord with the table, please contact your dealer immediately.

- Comtrend GS-7620 Smart-Lite PoE Switch or Comtrend GS-7624 Smart-Lite PoE Switch or Comtrend GS-7424 Smart-Lite Switch
- Quick Installation Guide
- Power Cord
- Manual CD
- Rack Mount Kit
- Foot pads

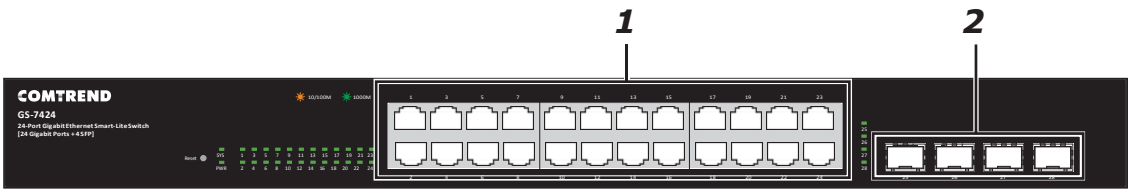
1.3. Features

- Supports PoE (GS-7620 and GS-7624) up to 30W per port with 330W total power budget
- Automatically detects powered devices (PD) and power consumption levels
- IEEE 802.1Q VLAN allows network segmentation to enhance performance and security
- Supports Access Control List (ACL)
- Switch capacity: GS-7624 & GS-7424: 56Gbps; GS-7620: 40Gbps, Forwarding rate: 35.7Mbps
- Supports IGMP Snooping V1 / V2 / partial V3
- 8K MAC address table and 9K jumbo frames

1.4. Product Components

1.4.1. Switch Views

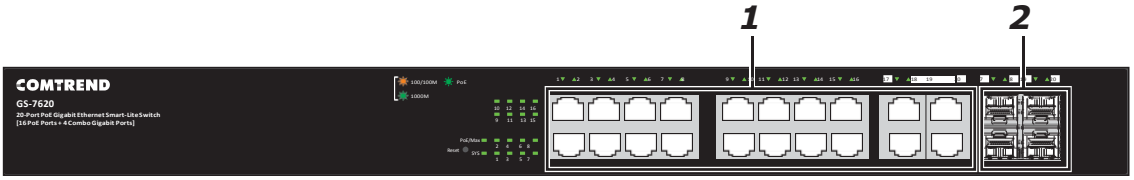
The following view applies to GS-7424.



Front View

No.	Name	Description
1	10/100/1000Mbps RJ-45 ports (1~24)	Designed to connect to network devices with a bandwidth of 10Mbps, 100Mbps or 1000Mbps. Each has a corresponding 10/100/1000Mbps LED.
2	SFP slots(SFP1,SFP2, SFP3, and SFP4)	Designed to install SFP modules and connect to network devices with a bandwidth of 1000Mbps. Each has a corresponding 1000Mbps LED.

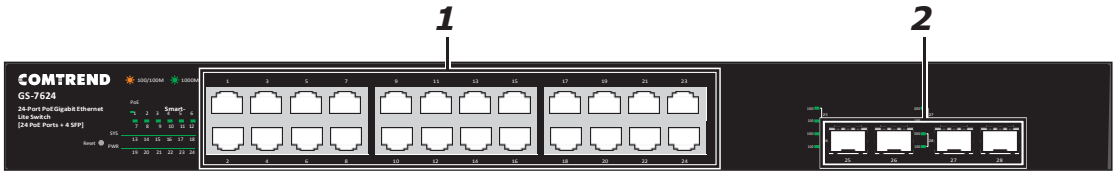
The following view applies to GS-7620.



Front View

No.	Name	Description
1	10/100/1000Mbps RJ-45 ports (1~20)	Designed to connect to network devices with a bandwidth of 10Mbps, 100Mbps or 1000Mbps. Each has a corresponding 10/100/1000Mbps LED.
2	SFP slots (SFP1, SFP2, SFP3, and SFP4)	Designed to install SFP modules and connect to network devices with a bandwidth of 1000Mbps. Each has a corresponding 1000Mbps LED.

The following view applies to GS-7624.



Front View

No.	Name	Description
1	10/100/1000Mbps RJ-45 ports (1~24)	Designed to connect to network devices with a bandwidth of 10Mbps, 100Mbps or 1000Mbps. Each has a corresponding 10/100/1000Mbps LED.
2	SFP ports (SFP1, SFP2, SFP3, and SFP4)	Designed to install SFP modules and connect to network devices with a bandwidth of 1000Mbps. Each has a corresponding 1000Mbps LED.

The following view applies to GS-7424, GS-7620, and GS-7624.

Rear View

No.	Name	Description
1	AC LINE	Supports AC 100 – 240V, 50-60Hz.

1.4.2. LED Indicators

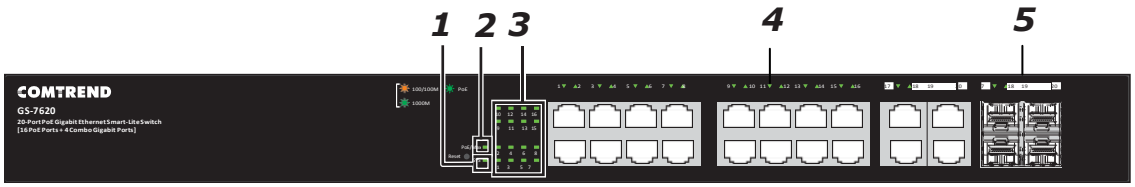
The following view applies to GS-7424.

Front View LED Indicators

No.	Name	Description
1	PWR	• Off: power off • On: power on
2	SYS	• Off: system not ready • On: system ready • Blinking: system boot-up

No.	Name	Description
3	Port LED LINK/ACT	Bi-color LED: • Off: port disconnected or link fail • Green On/Blinking: 1000Mbs connected/data transmitting • Amber On/Blinking: 10/100Mbs connected/data transmitting
4	SFP	• Off: port disconnected or link fail • Green On/Blinking: 1000Mbs connected/data transmitting

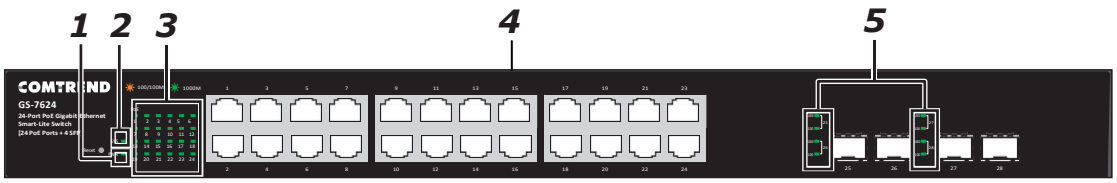
The following view applies to GS-7620.



Front View LED Indicators

No.	Name	Description
1	SYS	Green LED: • Off: power off or fail • On: power on • Blinking: system boot-up
2	PoE/Max	Green LED • Off: PoE power output under 320W PoE power budget • On: PoE power output over 320W PoE power budget
3	Port LED PoE	Green LED • Off: PoE power output off • On: PoE power output on
4	Port LED LINK/ACT	Bi-color LED: • Off: port disconnected or link fail • Green On/Blinking: 1000Mbs connected/data transmitting • Amber On/Blinking: 10/100Mbs connected/data transmitting
5	SFP	• Off: port disconnected or link fail • Green On/Blinking: 1000Mbs connected/data transmitting

The following view applies to GS-7624.



Front View LED Indicators

No.	Name	Description
1	PWR	• Off: power off • On: power on
2	SYS	• Off: system not ready • On: system ready • Blinking: system boot-up
3	Port LED PoE	Green LED • Off: PoE power output off • On: PoE power output on
4	Copper port LED: per port 2 LEDs, on RJ45 phone jack	• Green (right side): 1000Mbs connected • Yellow (left side): 10/100Mbs connected • Blinking: sending or receiving data • Off: port disconnected or link fail
5	SFP LED	• Off: port disconnected or link fail • Green On/Blinking: 1000Mbs connected/data transmittin

2. Installation

This chapter describes how to install and connect your Comtrend Switch. Read the following topics and perform the procedures in the correct order. Incorrect installation may cause damage to the product.

2.1. Mounting the Switch

There are two ways to physically set up the switch.

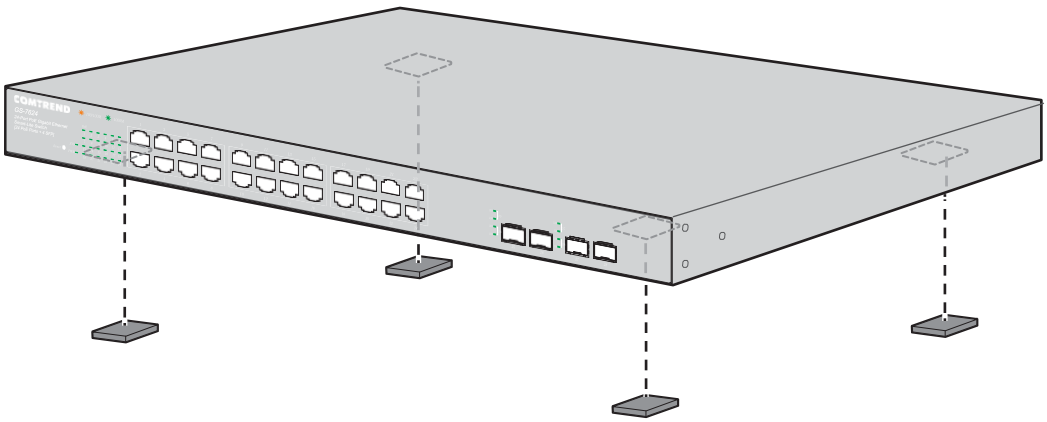
- Place the switch on a flat surface. To place the switch on a desktop, install the four rubber feet (included) on the bottom of the switch.
- Mount the switch in a standard rack (1 rack unit high).

2.1.1. Placement Tips

- Ambient Temperature—To prevent the switch from overheating, do not operate it in an area that exceeds an ambient temperature of 122°F (50°C).
- Air Flow—Be sure that there is adequate air flow around the switch.
- Mechanical Loading—Be sure that the switch is level and stable to avoid any hazardous conditions.
- Circuit Overloading—Adding the switch to the power outlet must not overload that circuit.

Follow these guidelines to install the switch securely.

1. Put the switch in a stable place such as a desktop, to avoid it falling.
2. Ensure the switch works in the proper AC input range and matches the voltage labeled.
3. Ensure there is proper heat dissipation from and adequate ventilation around the switch.
4. Ensure the switch's location can support the weight of the switch and its accessories.



Desktop Installation

2.1.2. Rack Mounting

You can mount the switch in any standard size, 19-inch (about 48 cm) wide rack. The switch requires 1 rack unit (RU) of space, which is 1.75 inches (44.45 mm) high.

For stability, load the rack from the bottom to the top, with the heaviest devices on the bottom. A top-heavy rack is likely to be unstable and may tip over.

When mounting smaller switch products into a standard 19-inch rack, a pair of extension brackets (sometimes referred to as ears) are needed to adapt the switch to the rack size.

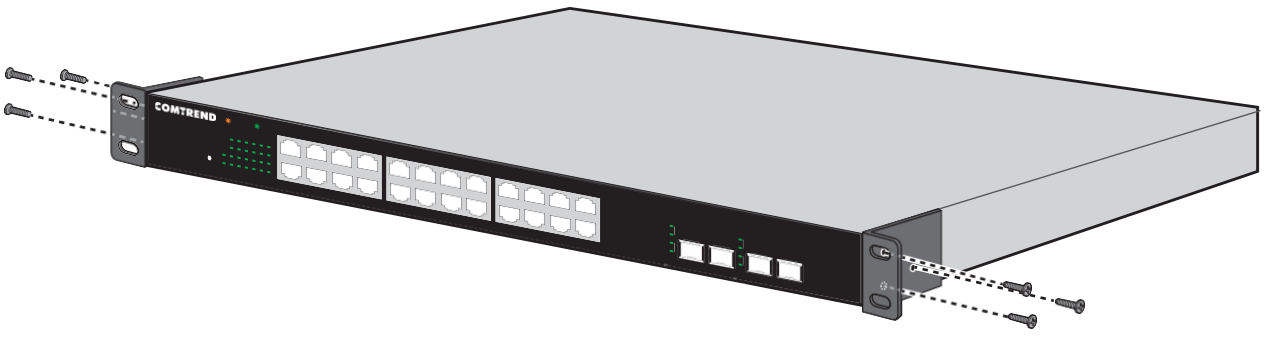
These extension brackets are mounted on the switch using the screws provided in the kit, and have two holes that are used to then screw the switch into the rack.

An example of one type of these extension brackets is shown in the following figure.

A common problem that occurs during rack mounting is the distance between the screw holes on the rack. Some racks are made with a uniform distance between all of the holes, and others have the holes organized into groups (see photo on the next page for an example).

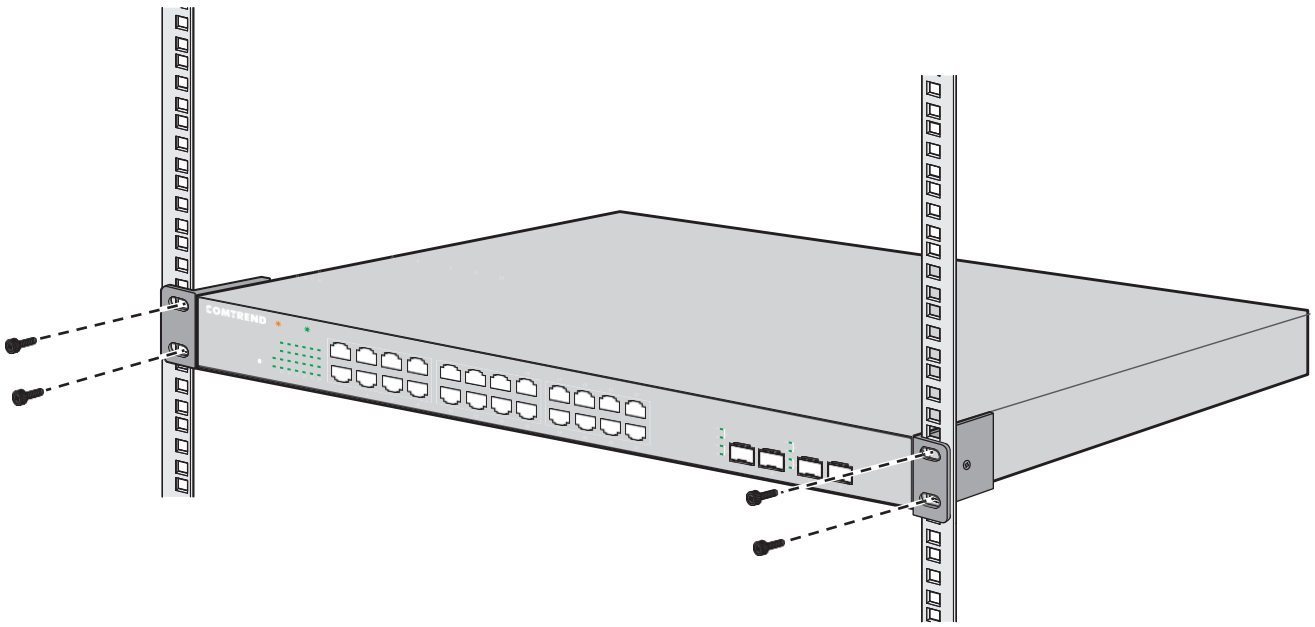
When organized into groups, the switch must be placed in the rack so that the holes in the extension brackets line up correctly.

1. Align the mounting brackets with the mounting holes on the switch's side panels and secure the brackets with the screws provided.



Bracket Installation

2. Secure the switch on the equipment rack with the screws provided.



Rack Installation

3. Getting Started

This section provides an introduction to the web-based configuration utility, and covers the following topics:

- Powering on the device
- Connecting to the network
- Power over Ethernet (PoE) considerations
- Starting the web-based configuration utility

3.1. Power

3.1.1. Connecting to Power

Power down and disconnect the power cord before servicing or wiring a switch.

Do not disconnect modules or cabling unless the power is first switched off. The device only supports the voltage outlined in the type plate. Do not use any other power components except those specifically designated for the switch.

Disconnect the power cord before installation or cable wiring.

The switch is powered by the AC 100-240 V 50/60Hz internal high-performance power supply. It is recommended to connect the switch with a single-phase three-wire power source with a neutral outlet, or a multifunctional computer professional source.

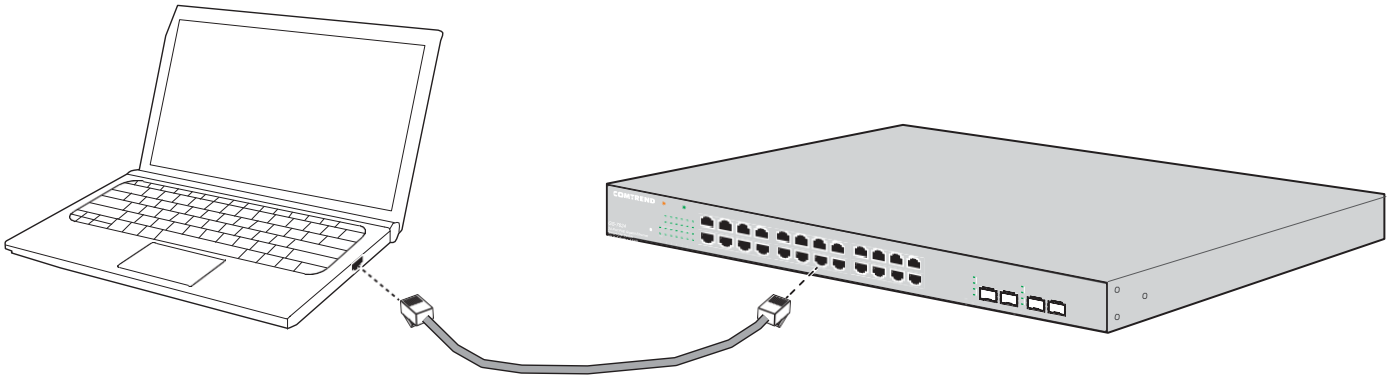
Connect the AC power connector on the back panel of the switch to the external power source with the included power cord, and check the power LED is on.

Rear View AC Power Socket

3.1.2. Connecting to the Network

To connect the switch to the network:

1. Connect an Ethernet cable to the Ethernet port of a computer
2. Connect the other end of the Ethernet cable to one of the numbered Ethernet ports of the switch. The LED of the port lights if the device connected is active.
3. Repeat Step 1 and Step 2 for each device to connect to the switch.
4. Connect the switch to end nodes using a standard Cat 5/5e Ethernet cable (UTP/STP) to connect the switch to end nodes as shown in the illustration below.
5. Switch ports will automatically adjust to the characteristics (MDI/MDI-X, speed, duplex) of the device to which the switch is connected.



PC Connect

3.1.3. Power over Ethernet (PoE) Considerations

For PoE switch models, consider the following information:

Devices considered a Power Sourcing Equipment (PSE), can support up to 30 Watts per PoE port.

Model	Power Dedicated to PoE	PoE Ports	PoE Standard Supported
GS-7620	330W	1 to 16	IEEE802.3at/af
GS-7624	330W	1 to 24	IEEE802.3at/af

Ports 1-24 provide PoE power supply functionality with a maximum output power up to 30W each port. This can supply power to PDs such as internet phones, network cameras, wireless access points. Connect the switch PoE port directly to the PD port using a network cable.

When connecting switches capable of supplying PoE, consider the following information:

- Switch models with PoE function are PSEs. These models are capable of supplying DC power to attached PDs, such as VoIP phones, IP cameras, and wireless access points (APs). PoE switches. Additionally, PoE switches are capable of detecting and supplying power to pre-standard legacy PoE Power Devices. Due to the support for legacy PoE, there is a possibility that PoE switches acting as a PSE may inadvertently detect and supply power an attached PSE, including other PoE switches. This false detection may result in a PoE switch operating improperly and unable to supply power to attached PDs.
- The prevention of a false detection can be easily remedied by disabling PoE on the ports that are used to connect PSEs. Another simple practice to prevent a false detection is to first power up a PSE device before connecting it to a PoE switch.
- When a device is falsely detected as a PD, disconnect the device from the PoE port and power recycle the device with AC power before reconnecting it to the PoE port.

3.1.4. Starting the Web-based Configuration Utility

This section describes how to navigate the web-based switch configuration utility.

Be sure to disable any pop-up blocker.

Browser Restrictions

- If you are using older versions of Internet Explorer, you cannot directly use an IPv6 address to access the device. You can, however, use the DNS (Domain Name System) server to create a domain name that contains the IPv6 address, and then use that domain name in the address bar in place of the IPv6 address.
- If you have multiple IPv6 interfaces on your management station, use the IPv6 global address instead of the IPv6 link local address to access the device from your browser.

Launching the Configuration Utility

To open the web-based configuration utility:

1. Open a Web browser.
2. Enter the IP address of the device you are configuring in the address bar on the browser (factory default IP address is 192.168.169.1) and then press Enter.

Your computer's IP address must be in the same subnet as the switch. For example, if the switch is using the factory default IP address, your computer's IP address can be in the following range: 192.168.169.x (whereas x is a number from 2 to 254).

After a successful connection, the login window displays.

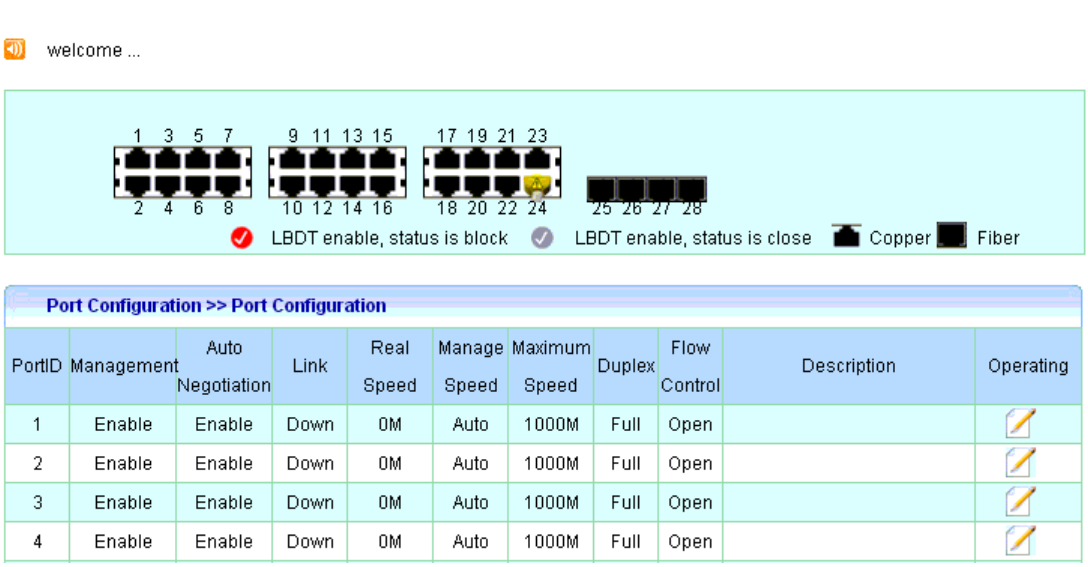
Login Window

3.1.5. Logging In

To log in to the device configuration utility:

1. Enter the default user ID (admin) and the default password (admin).
2. If this is the first time that you logged on with the default user ID (admin) and the default password (admin). It is recommended that you change your password immediately. See “4.9.3. Administrator” on page 79 for additional information.

When the login attempt is successful, the **Port Configuration** window displays.



PortID	Management	Auto Negotiation	Link	Real Speed	Manage Speed	Maximum Speed	Duplex	Flow Control	Description	Operating
1	Enable	Enable	Down	0M	Auto	1000M	Full	Open		
2	Enable	Enable	Down	0M	Auto	1000M	Full	Open		
3	Enable	Enable	Down	0M	Auto	1000M	Full	Open		
4	Enable	Enable	Down	0M	Auto	1000M	Full	Open		

Port Configuration

If you entered an incorrect username or password, an error message appears and the Login page remains displayed on the window. If you are having problems logging in, please see the “Launching the Configuration Utility” section in the User Manual for additional information.

Logging Out

By default, the application logs out after ten minutes of inactivity.

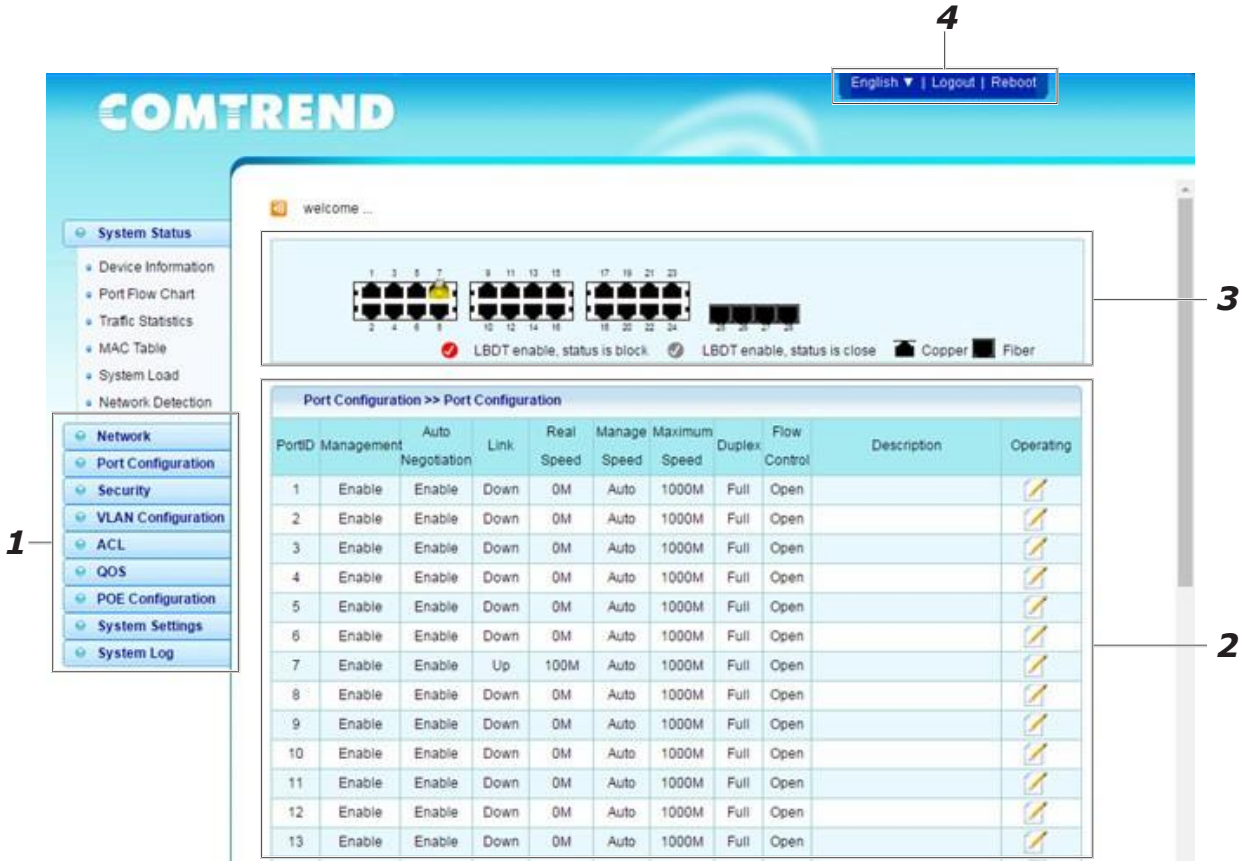
To logout, click Logout in the top right corner of any page. The system logs out of the device.

When a timeout occurs or you intentionally log out of the system, the Login page appears. After you log in, the application returns to the initial page.

4. Web-based Switch Configuration

The PoE smart switch software provides rich functionality for switches in your networks. This chapter describes how to use the web-based management interface (Web UI) to configure the switch's features.

For the purposes of this manual, the user interface is separated into four sections, as shown in the following figure:



User Interface

No.	Name	Description
1	Configuration menu	Navigate to locate specific switch functions.
2	Configuration settings	Edit specific function settings.
3	Switch's current link status	Green squares indicate the port link is up, while black squares indicate the port link is down.
4	Common toolbar	Provides access to frequently used settings.

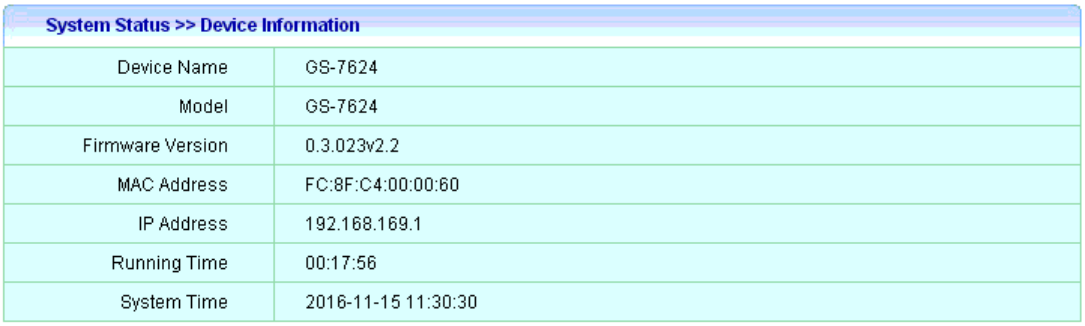
4.1. System Status

View device information and status.

4.1.1. Device Information

Use this page to view status information such as Device ID, MAC address, IP Address and System Time.

To view the Device Information menu, navigate to System Status > Device Information.



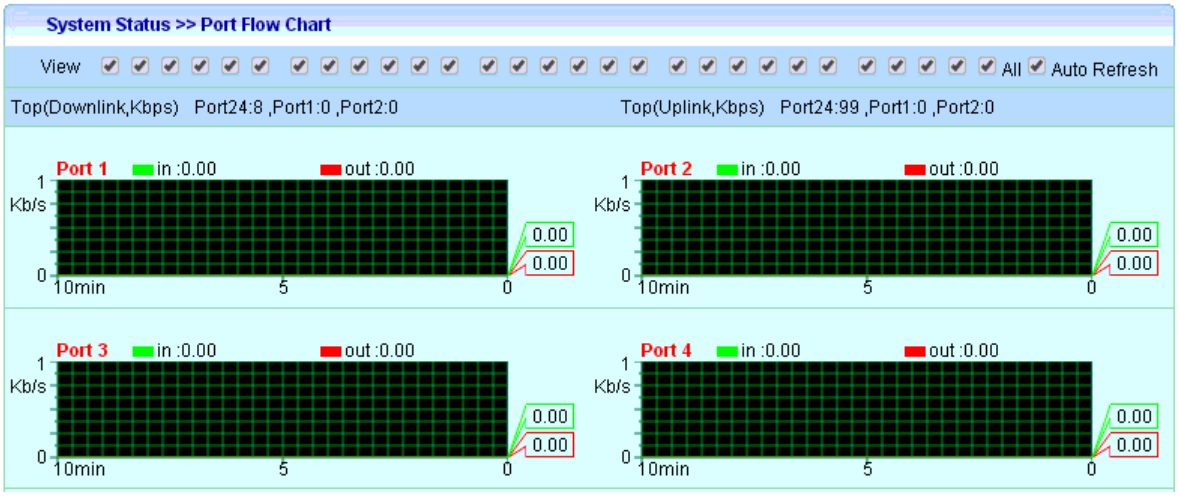
System Status > Device Information

Item	Description
Device Name	System name of the switch, configurable according to user preference.
Model	Switch model name.
Firmware Version	Current firmware version of the device.
MAC Address	A unicast MAC address for which the switch has forwarding and/or filtering information. The format is a six-byte MAC address, with each byte separated by colons.
IP Address	Switch IP address on the network.
Running Time	Duration switch has been running since last reset or power off.
System Time	Current date and time as reported by the system.

4.1.2. Port Flow Chart

Use this page to view port flow information such as port uplink and downlink usage, and enable or disable Port Admin State.

To view the Port Flow Chart menu, navigate to System Status > Port Flow Chart.



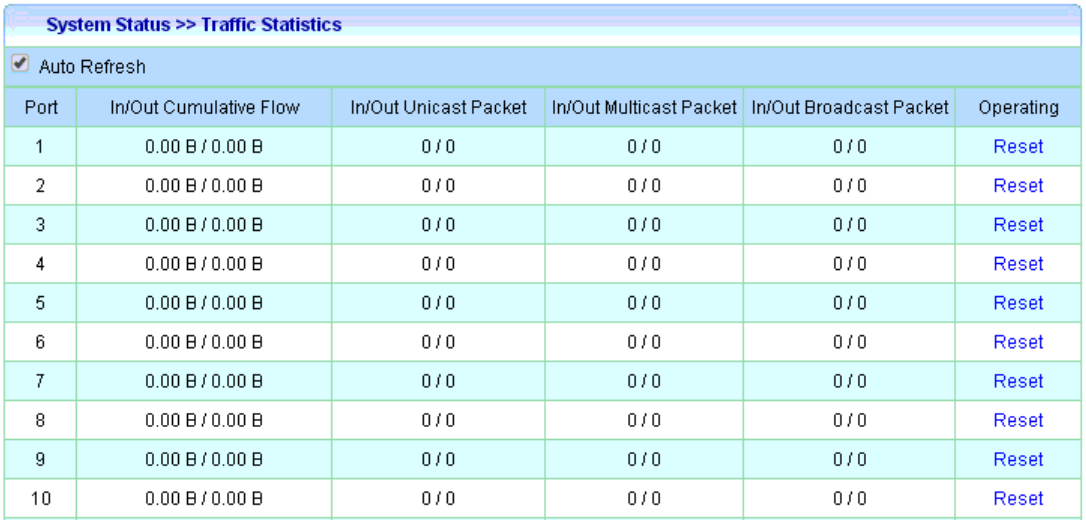
System Status > Port Flow Chart

Item	Description
View	Select which ports to view.
Auto Refresh	Automatically update data display periodically.

4.1.3. Traffic Statistics

Use this page to view traffic information such as Cumulative Flow, Unicast Packets, Multicast Packets and Broadcast Packets on each port. The tracking data on each port can also be reset.

To view the Traffic Statistics menu, navigate to System Status > Traffic Statistics.



System Status > Traffic Statistics

Item	Description
Auto Refresh	Automatically update data display periodically.
Port	Number of port being monitored.
In/Out Cumulative Flow	The total number of packets including unicast, broadcast, and multicast packets, successfully transmitted or received by the processor.
In/Out Unicast Packet	The number of subnetwork-unicast packets delivered to or received from a higher-layer protocol.
In/Out Multicast Packet	The total number of packets transmitted or received by the device that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
In/Out Broadcast Packet	The total number of packets transmitted or received by the device that were directed to the broadcast address. Note that this number does not include multicast packets.
Operating	Use this option to reset the tracking data of a port.

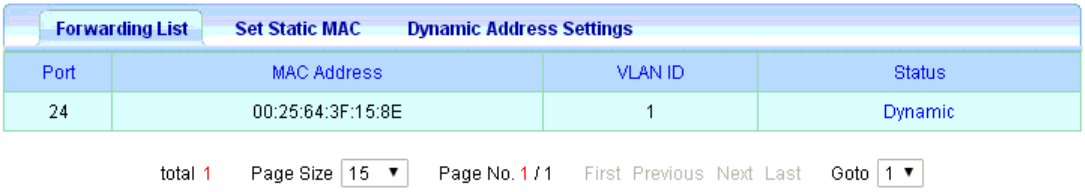
4.1.4. MAC Table

Use this section to configure a relationship between a MAC address, VLAN ID and switch port. The MAC address table keeps track of the Media Access Control (MAC) addresses that are associated with each port. This table allows the device to forward unicast traffic through the appropriate port.

The MAC address table is sometimes called the bridge table or the forwarding database. Use the MAC Address Table page to display information about entries in the MAC address table.

Forwarding List

To view the Forwarding List menu, navigate to System Status > MAC Table > Forwarding List.

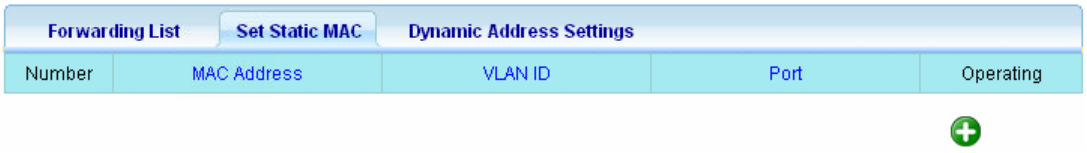


System Status > MAC Table > Forwarding List

Item	Description
Port	Designated port number.
MAC Address	A unicast MAC address for which the switch has forwarding and/or filtering information. The format is a six-byte MAC address, with each byte separated by colons.
VLAN ID	The VLAN with which the MAC address is associated. A MAC address can be associated with multiple VLANs.
Status	Provides information about the entry and why it is in the table. Click on the entry to configure the status: • Static: The address has been manually configured and does not age out • Dynamic: The address has been automatically learned by the device and can age out when it is not in use.

Set Static MAC

To view the Set Static MAC menu, navigate to System Status > MAC Table > Set Static MAC.

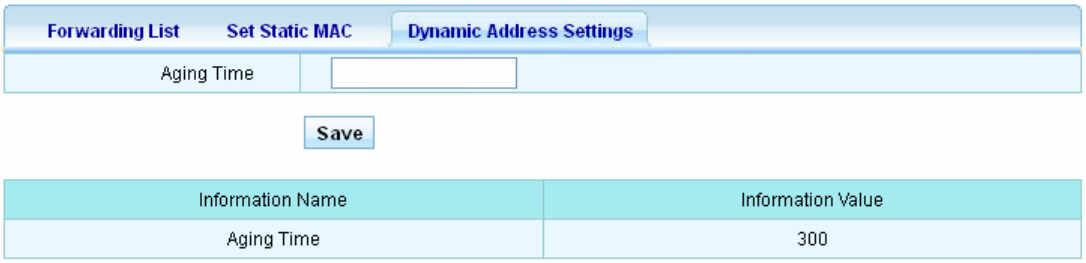


System Status > MAC Table > Set Static MAC

Item	Description
MAC Address	A unicast MAC address for which the switch has forwarding and/or filtering information. The format is a six-byte MAC address, with each byte separated by colons.
VLAN ID	The VLAN with which the MAC address is associated. A MAC address can be associated with multiple VLANs.
Port	Designated port number.
Operating	Use this option to add static entries to the MAC address table by entering the following data: • MAC address • VLAN ID • Port number

Dynamic Address Settings

To view the Dynamic Address Settings menu, navigate to System Status > MAC Table > Dynamic Address Settings.



System Status > MAC Table > Dynamic Address Settings

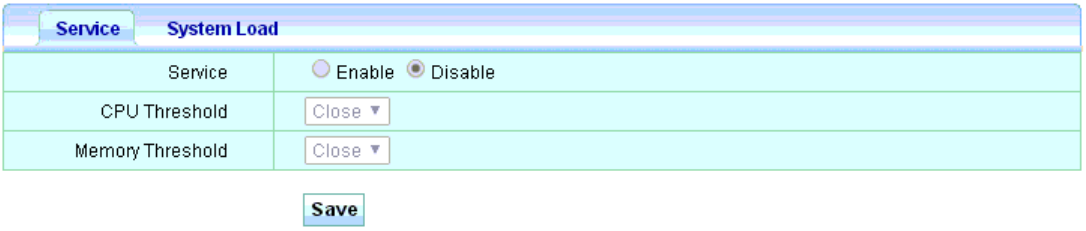
Item	Description
Aging Time (seconds)	Enter the amount of time, in seconds, that a dynamic ARP entry should remain in the ARP table before aging out.
Save	Click **Save** to save the values and update the screen.

4.1.5. System Load

Use this section to configure the Maximum CPU/Memory Threshold. The Service tab enables and disables this feature, and sets the threshold parameter. The System Load tab provides a view of system resource usage over the last 10 minutes.

Service

To view the Service menu, navigate to System Status > System Load > Service.

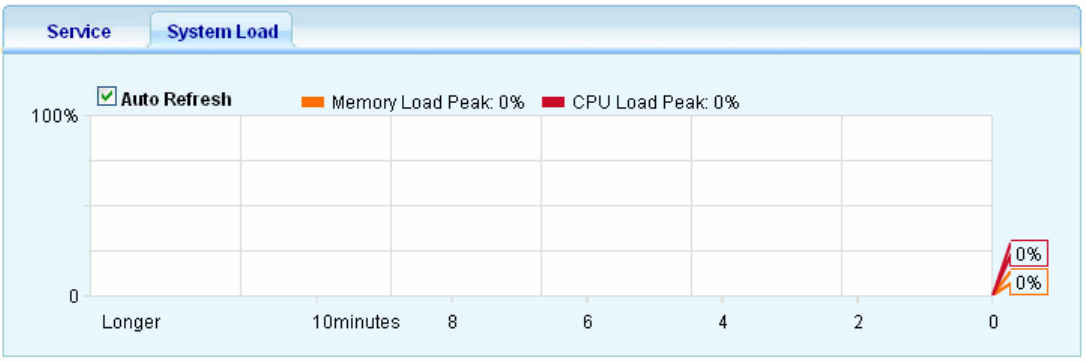


System Status > System Load > Service

Item	Description
Service	Enable/disable the system load service.
CPU Threshold	Set the CPU load threshold.
Memory Threshold	Set the memory load threshold.
Save	Click **Save** to save the values and update the screen.

System Load

To view the System Load menu, navigate to System Status > System Load > System Load.



System Status > System Load > System Load

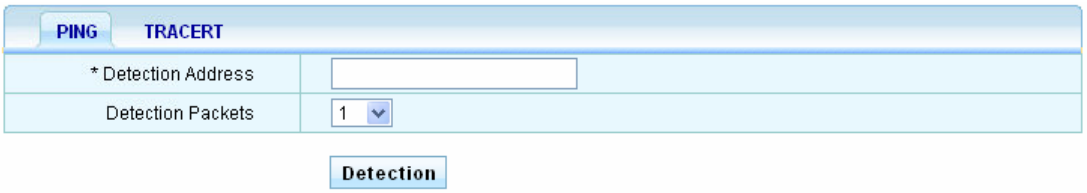
Item	Description
Auto Refresh	Automatically update data display periodically.

4.1.6. Network Detection

This section has two tools for network connection confirmation. The Ping tool has a field to input the ping destination along with a dropdown to indicate how many attempts to make. The Tracert tool has a destination address and dropdown to indicate how many hops to report.

Ping

To view the Ping menu, navigate to System Status > Network Detection > Ping.

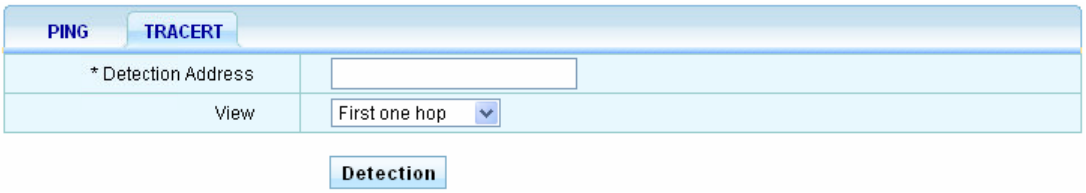


System Status > Network Detection > Ping

Item	Description
Detection Address	Enter the IP address to be pinged.
Detection Packets	Enter the number of packets to be used in the ping.
Detection	Click **Detection** to execute ping command.

Tracert

To view the Tracert menu, navigate to System Status > Network Detection > Tracert.



System Status > Network Detection > Tracert

Item	Description
Detection Address	Enter the IP address to be traced.
View	Select the number of hops to be viewed.
Detection	Click **Detection** to execute tracert command.

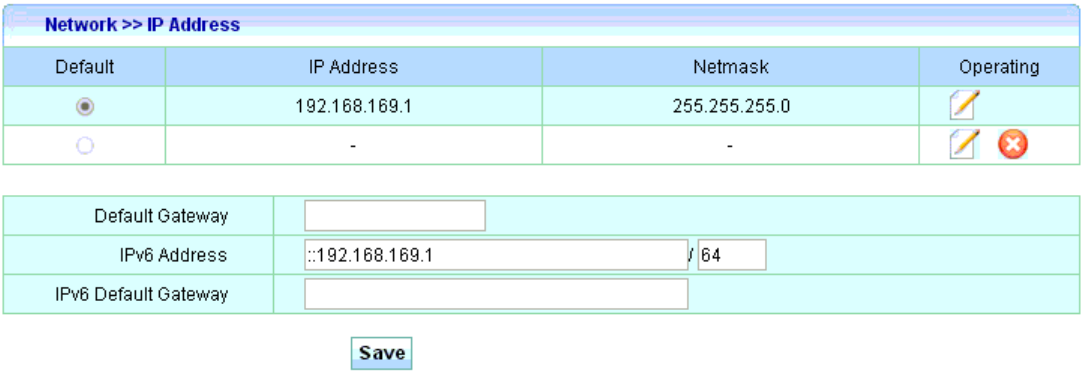
4.2. Network

Use the Network pages to configure settings for the switch network interface and connections to a remote server.

4.2.1. IP Address

This section allows you to edit the IP address, Netmask and Gateway of the switch.

To view the IP Address menu, navigate to Network > IP Address.



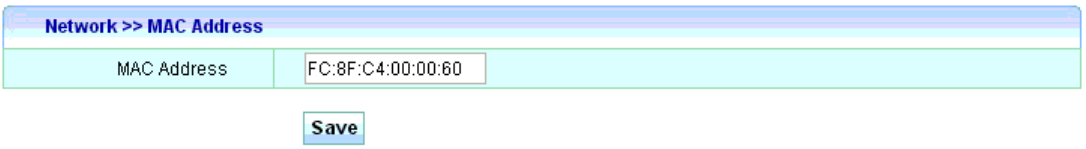
Network > IP Address

Item	Description
IP Address	If static mode is enabled, enter IP address in this field.
Netmask	If static mode is enabled, enter subnet mask in this field.
Operating	Click to configure IP address settings by entering the following data: • IP address • Netmask
Default Gateway	A Gateway Address is chosen to be the address of a router that connects two different networks.
IPv6 Address	Enter the IPv6 address of the switch.
IPv6 Default Gateway	The default gateway for the IPv6 network interface.
Save	Click **Save** to save the values and update the screen.

4.2.2. MAC Address

Use this section to edit the MAC address of the switch.

To view the MAC Address menu, navigate to Network > MAC Address.



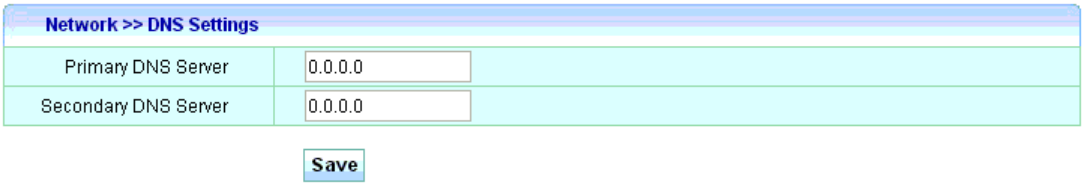
Network > MAC Address

Item	Description
MAC Address	Select the MAC address to show or clear dynamic MAC entries. If no port, VLAN and MAC address is selected, the dynamic MAC table will be cleared.
Save	Click **Save** to save the values and update the screen.

4.2.3. DNS Settings

Use this section to edit the DNS Server(s) for the switch.

To view the DNS Settings menu, navigate to Network > DNS Settings.



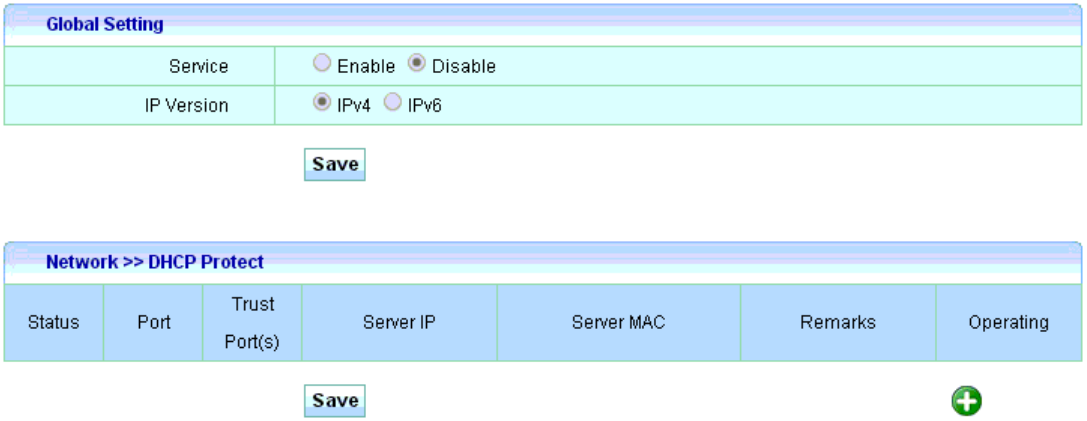
Network > DNS Settings

Item	Description
Primary DNS Server	The IP addresses of a primary DNS server the client should use to resolve host names into IP addresses.
Secondary DNS Server	The IP addresses of a secondary DNS server the client should use to resolve host names into IP addresses.
Save	Click **Save** to save the values and update the screen.

4.2.4. DHCP Protect

When the switch uses DHCP Protect, it will snoop protect message and DHCP requests and record the IP address and MAC address from DHCP ACK messages. DHCP Protect allows physical ports to be set as creditable ports or discreditable ports. Creditable ports can receive and forward the DHCP offer message while discreditable port will lose the DHCP offer message. This is so the switch can identify false DHCP servers and ensure that the client gets an IP address from the DHCP Server.

To view the DHCP Protect menu, navigate to Network > DHCP Protect.



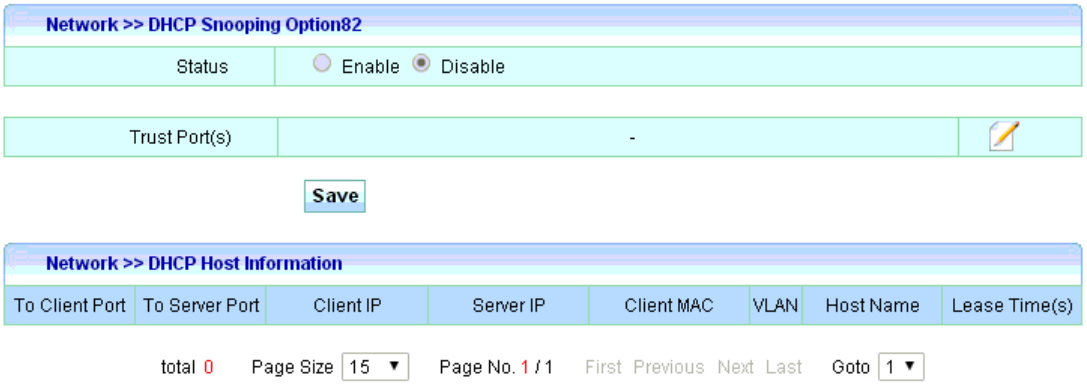
Network > DHCP Protect

Item	Description
Global Setting	
Service	Enable/disable DHCP protection.
IP Version	Select the IP version of the network (IPv4 or IPv6).
Save	Click **Save** to save the values and update the screen.
Network >> DHCP Protect	
Operating	Click to add a protected port by entering the following data: • Service (enable or disable) • Port number • DCHP server IP address • DHCP server MAC address • Remarks
Save	Click **Save** to save the values and update the screen.

4.2.5. DHCP Snooping Option 82

Use this section to create a DHCP Snooping Option 82 Profile. When enabled, the device checks packets that are received on untrusted interfaces to verify that the MAC address and the DHCP client hardware address match. If the addresses do not match, the device drops the packet.

To view the DHCP Snooping Option 82 menu, navigate to Network > DHCP Snooping Option 82.



Network > DHCP Option 82

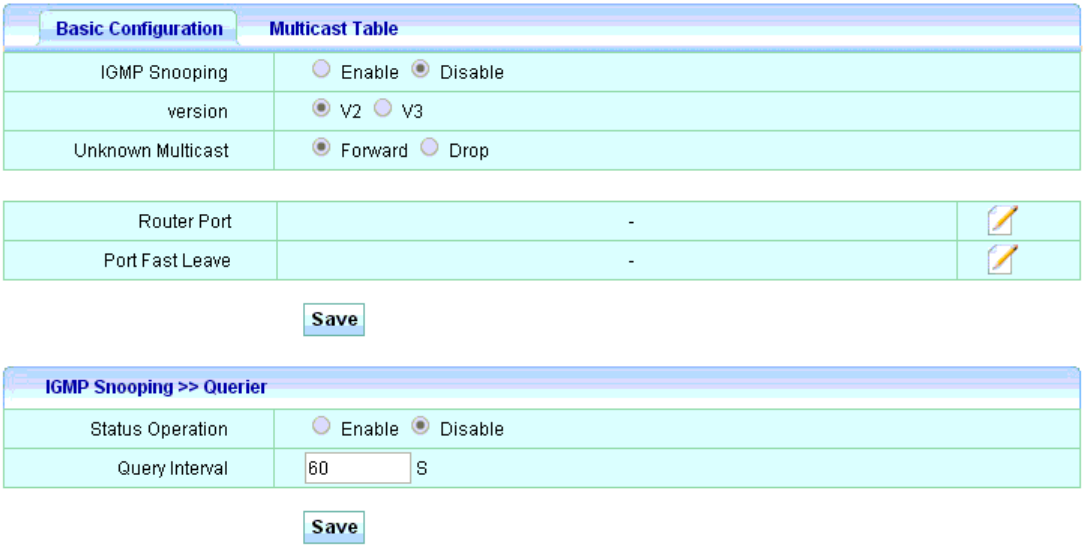
Item	Description
Status	Enable/disable DHCP snooping.
Trust Port(s)	Click to select ports to add to the trust list.
Save	Click **Save** to save the values and update the screen.

4.2.6. IGMP Snooping

Use this section to create an IGMP Snooping Profile. Internet Group Management Protocol (IGMP) Snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch. Multicast IP traffic is traffic that is destined to a host group. Host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request the multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly affecting network performance.

Basic Configuration

To view the Basic Configuration menu, navigate to Network > IGMP Snooping > Basic Configuration.



Network > IGMP Snooping > Basic Configuration

Item	Description
Basic Configuration	
IGMP Snooping	Enable/disable IGMP snooping.
Version	Select IGMP version 2 or IGMP version 3.
Unknown Multicast	Select whether to forward or drop unknown multicast packets.
Router Port	Configure the router port by selecting ports.
Port Fast Leave	Configure the port fast leave settings by selecting ports.
Save	Click **Save** to save the values and update the screen.
IGMP Snooping >> Querier	
Status Operation	Enable/disable IGMP snooping querier.
Query Interval	Enter a value representing the delay in seconds the IGMP snooping querier sends out IGMP queries.
Save	Click **Save** to save the values and update the screen.

Multicast Table

To view the Multicast Table menu, navigate to Network > IGMP Snooping > Multicast Table.

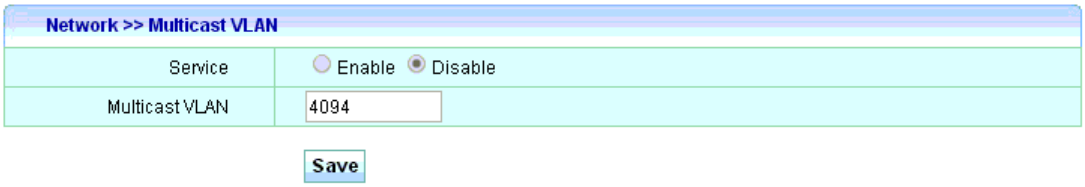
Network > IGMP Snooping > Multicast Table

Item	Description
Multicast IP	Multicast IP address.
VLAN ID	Virtual LAN ID.
Port	Designated port number.
Operating	Use this option to add entries to the multicast table by entering the following data: • Multicast IP address • VLAN ID • Port number

4.2.7. Multicast VLAN

Use this section to enable Multicast VLAN and specify the appropriate port.

To view the Multicast VLAN menu, navigate to Network > Multicast VLAN.



Network > Multicast VLAN

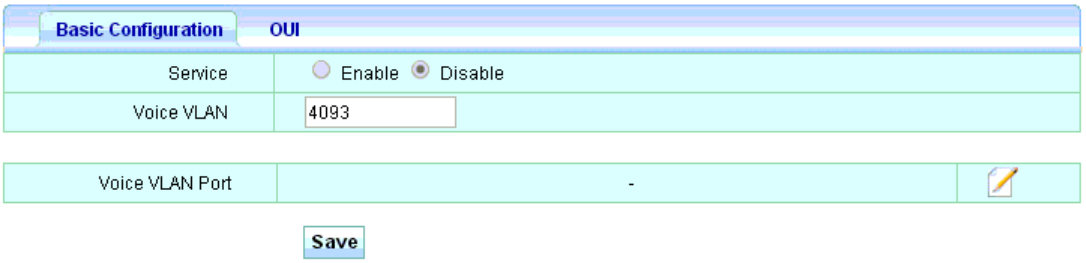
Item	Description
Service	Enable/disable multicast VLAN.
Multicast VLAN	Enter the multicast VLAN port address.
Save	Click **Save** to save the values and update the screen.

4.2.8. Voice LAN

Use this section to create VLANs to group and prioritize voice traffic.

Basic Configuration

To view the Basic Configuration menu, navigate to Network > Voice VLAN > Basic Configuration.



Network > Voice VLAN > Basic Configuration

Item	Description
Service	Enable/disable voice VLAN.
Voice VLAN	Enter the voice VLAN port number.
Voice VLAN Port	Configure the voice VLAN port settings by selecting ports.
Save	Click **Save** to save the values and update the screen.

OUI

To view the OUI menu, navigate to Network > Voice VLAN > OUI.

Network > Voice VLAN > OUI

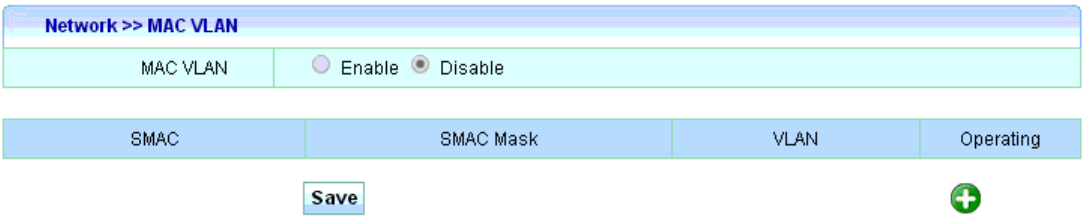
Item	Description
Number	Voice VLAN port number.
OUI	Organizationally Unique Identifier.
Company	Description of the OUI.

Item	Description
Operating	Click to add entries to the OUI list by entering the following data: • OUI MAC address • Company name
Save	Click **Save** to save the values and update the screen.

4.2.9. MAC VLAN

Use this section to create a MAC based VLAN. This will allow untagged packets to be assigned a VLAN without being tied to a specific switch port. This flexibility allows for a dynamic switch source port while maintaining the VLAN segregation based on the MAC address of the device.

To view the MAC VLAN menu, navigate to Network > MAC VLAN.



Network > MAC VLAN

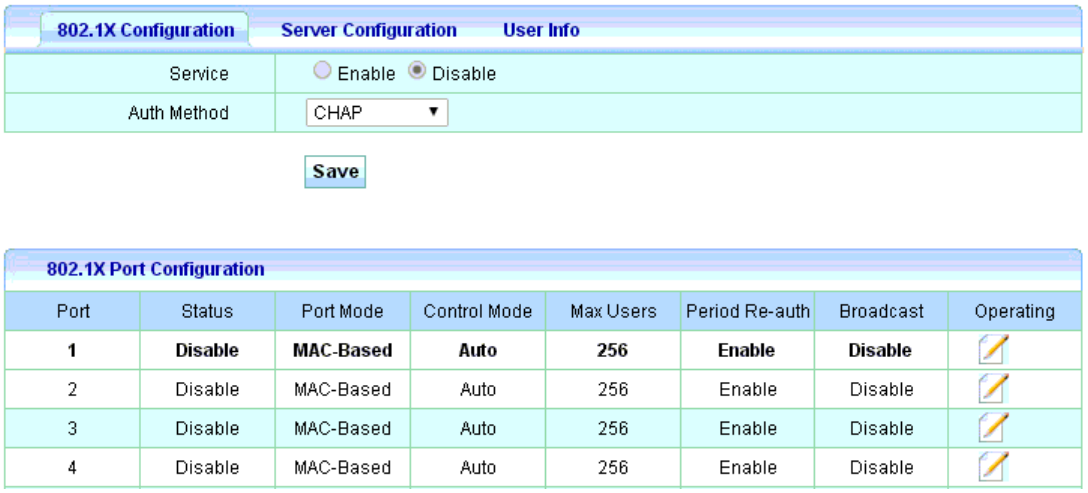
Item	Description
MAC VLAN	Enable/disable MAC VLAN.
SMAC	Smac MAC Address Changer, used to mask a MAC address.
SMAC Mask	Masked MAC address generated by SMAC.
VLAN	Designation for the VLAN entry.
Operating	Click to add entries to the MAC VLAN by entering the following data: • SMAC • SMAC Mask • VLAN ID
Save	Click **Save** to save the values and update the screen.

4.2.10. 802.1x

Use this section to enable/disable IEEE 802.1x security.

802.1x Configuration

To view the 802.1x Configuration menu, navigate to Network > 802.1x > 802.1x Configuration.



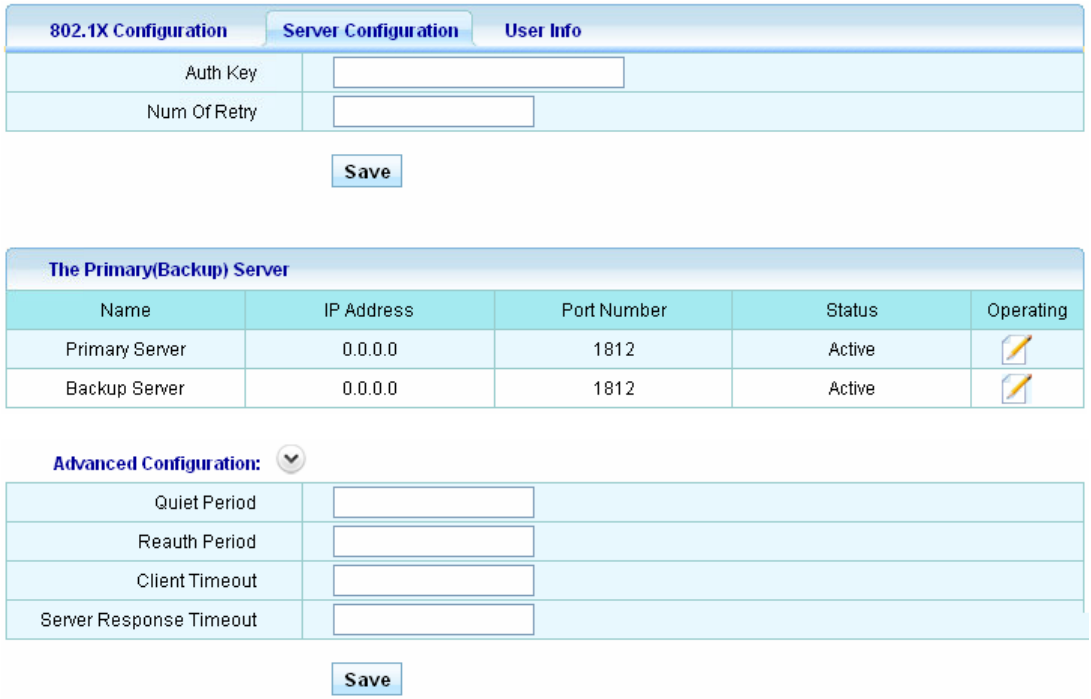
Network > 802.1x > 802.1x Configuration

Item	Description
802.1x Configuration	
Service	Enable/disable IEEE 802.1x security.
Auth Method	Select an authorization method: • EAP: Password Authentication Protocol • CHAP: Challenge-Handshake Authentication Protocol
Save	Click **Save** to save the values and update the screen.
802.1x Port Configuration	
Port	Designated port number.
Status	Displays whether port is enabled or disabled.
Port Mode	Displays port mode.

Item	Description
Control Mode	The port-based access control mode on the port, which is one of the following: • Auto: The port is unauthorized until a successful authentication exchange has taken place. • Force Unauthorized: The port ignores supplicant authentication attempts and does not provide authentication services to the client. • Force Authorized: The port sends and receives normal traffic without client port-based authentication. • MAC-Based: This mode allows multiple supplicants connected to the same port to each authenticate individually. Each host connected to the port must authenticate separately in order to gain access to the network. The hosts are distinguished by their MAC addresses.
Max Users	The maximum number of clients supported on the port if the Control Mode on the port is MAC-based 802.1x authentication.
Period Re-auth	The amount of time that clients can be connected to the port without being reauthenticated. If this field is disabled, connected clients are not forced to reauthenicate periodically.
Broadcast	Enable/disable broadcast.
Operating	Click to edit port configuration settings by entering the following data: • Port number • Status (enable, disable) • Port mode (MAC-based, Port-based) • Control mode (auto, force auth, force unauth) • Max users (1-256) • Period re-authentication (enable, disable) • Broadcast (enable, disable)

Server Configuration

To view the Server Configuration menu, navigate to Network > 802.1x > Server Configuration.



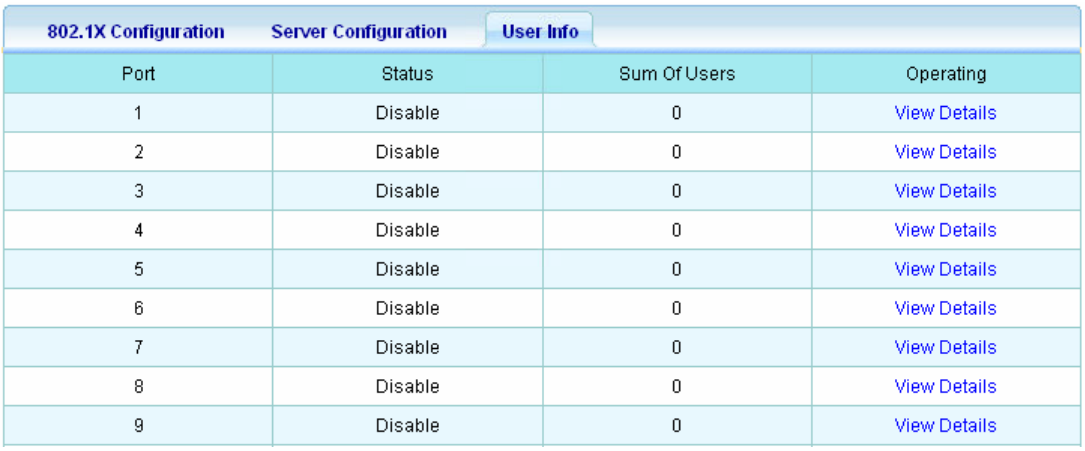
Network > 802.1x > Server Configuration

Item	Description
Server Configuration	
Auth Key	Specifies the password used to generate the key to be used in encrypting messages to and from this user.
Num of Retry	The number of times the DNS client should attempt to send DNS queries to a DNS server on the network.
Save	Click **Save** to save the values and update the screen.
The Primary(Backup) Server	
Name	Server name.
IP Address	IP address designation for entry.
Port Number	Designated port number for entry.
Status	Displays whether the server is active or inactive.
Operating	Click to edit server configuration settings by entering the following data: • IP address • Port number • Status (active, block)

Item	Description
Advanced Configuration	
Quiet Period	Enter the length of time for which the routing table remains frozen.
Reauth Period	Enter the amount of time that clients can be connected to the port without being reauthenticated. If this field is disabled, connected clients are not forced to reauthenicate periodically.
Server Response Timeout	Enter how the amount of time the server should wait for a response before timing out.

User Info

To view the User Info menu, navigate to Network > 802.1x > User Info.



Network > 802.1x > User Info

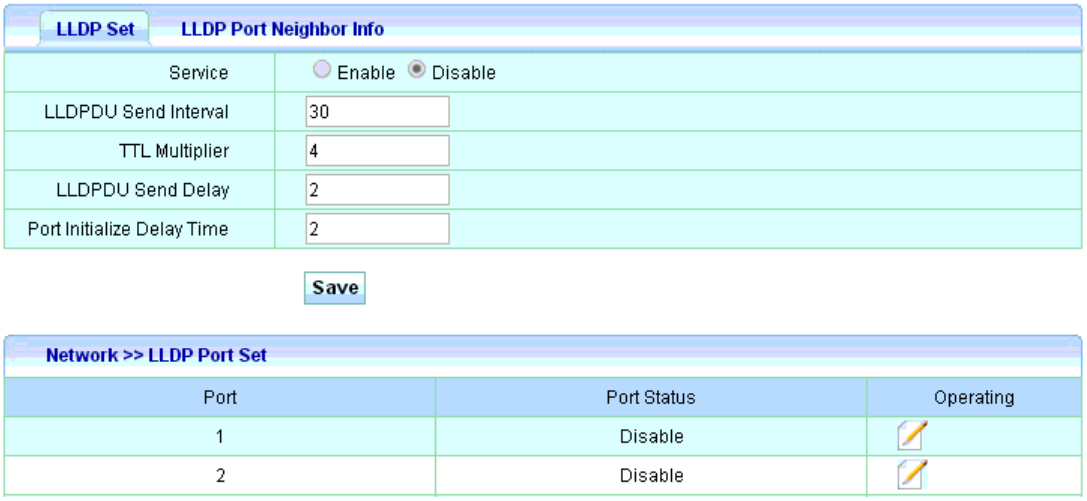
Item	Description
Port	Designated port number.
Status	Displays whether the port is enabled or disabled.
Sum of Users	Total number of users on the current port.
Operating	View selected port details.

4.2.11. LLDP

Use this section to enable/disable Link Layer Discovery Protocol (LLDP). This Layer 2 protocol can assist an Administrator discover network changes and manage reconfiguration maintenance by storing advertised network device information from adjacent network devices.

LLDP Set

To view the LLDP Set menu, navigate to Network > LLDP > LLDP Set.

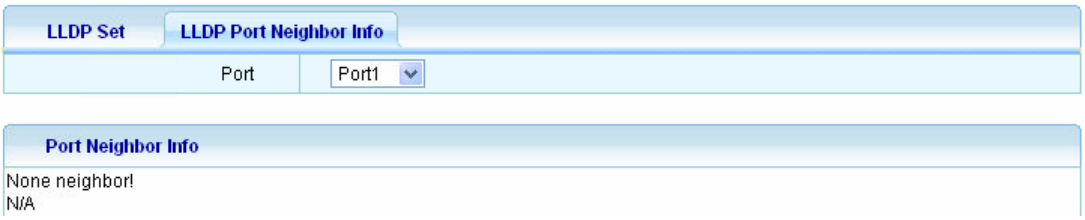


Network > LLDP > LLDP Set

Item	Description
LLDP Set	
Service	Enable/disable LLDP.
LLDPDU Send Interval	The number of seconds between transmissions of LLDP advertisements.
TTL Multiplier	The Transmit Interval multiplier value, where Transmit Hold Multiplier - Transmit Interval = the time to live (TTL) value the device advertises to neighbors.
LLDPDU Send Delay	The minimum number of seconds to wait between transmissions of remote data change notifications to the SNMP trap receiver(s) configured on the device.
Port Initialize Delay Time	Enter a value in seconds between reinitializing LLDP on a port after reconfiguring the setting.
Save	Click **Save** to save the values and update the screen.
Network >> LLDP Port Set	
Port	Designated port number.
Port Status	Displays whether the port is enabled or disabled.
Operating	Configure LLDP port settings by entering the following data: • Port status (enable, disable)

LLDP Port Neighbor Info

To view the LLDP Port Neighbor Info menu, navigate to Network > LLDP > LLDP Port Neighbor Info.



Network > LLDP > LLDP Port Neighbor Info

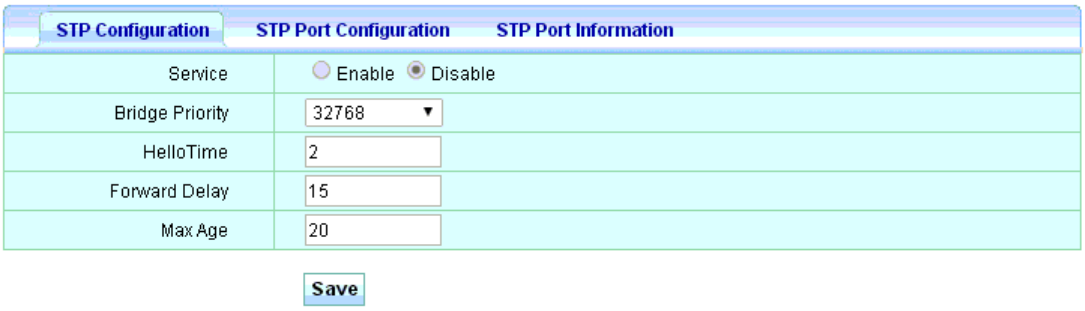
Item	Description
Port	Designated port number.
Port Neighbor Info	View information about the neighboring devices connected to each port.

4.2.12. STP

Use this section to enable/disable/configure Spanning Tree Protocol. The Spanning Tree Protocol (STP) provides a tree topology for any arrangement of bridges. STP also provides one path between end stations on a network, eliminating loops. Spanning tree versions supported include Common STP, Multiple STP, and Rapid STP.

STP Configuration

To view the STP Configuration menu, navigate to Network > STP > STP Configuration.



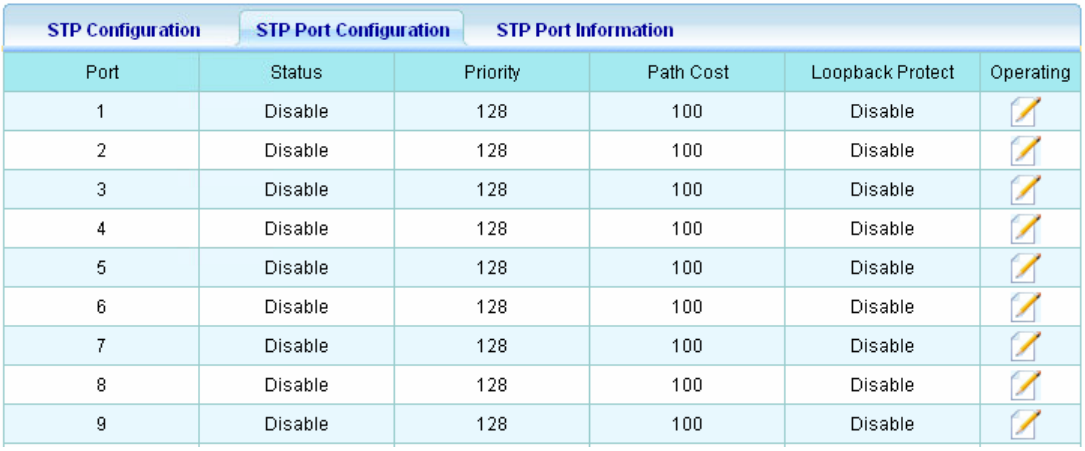
Network > STP > STP Configuration

Item	Description
Service	Enable/disable STP configuration.
Bridge Priority	Select which bridge is elected as the root bridge, and which bridge is elected as the root bridge when the initial root bridge fails.

Item	Description
HelloTime	Time between each bridge protocol data unit (BPDU) sent on a port.
Save	Click **Save** to save the values and update the screen.

STP Port Configuration

To view the STP Port Configuration menu, navigate to Network > STP > STP Port Configuration.

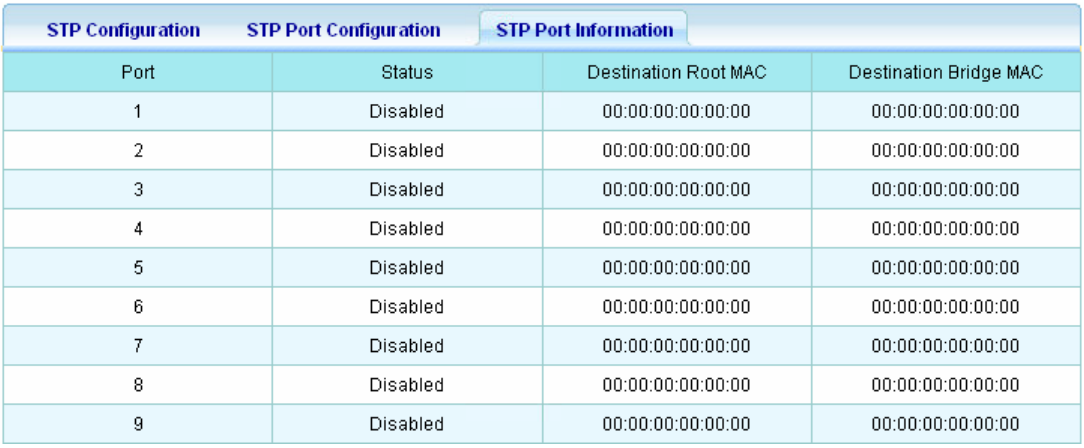


Network > STP > STP Port Configuration

Item	Description
Port	Designated port number.
Status	Displays whether the port is enabled or disabled.
Priority	The bridge priority for the spanning-tree instance. This value affects the likelihood that the bridge is selected as the root bridge. A lower value increases the probability that the bridge is selected as the root bridge.
Path Cost	The path cost from the port to the root bridge.
Loopback Protect	Displays whether loopback protection is enabled or disabled.
Operating	Click to configure STP Port Configuration settings by entering the following data: • Status (enable, disable) • Priority (0-240) • Path cost • Loopback protect (enable, disable)

STP Port Information

To view the STP Port Information menu, navigate to Network > STP > STP Port Information.



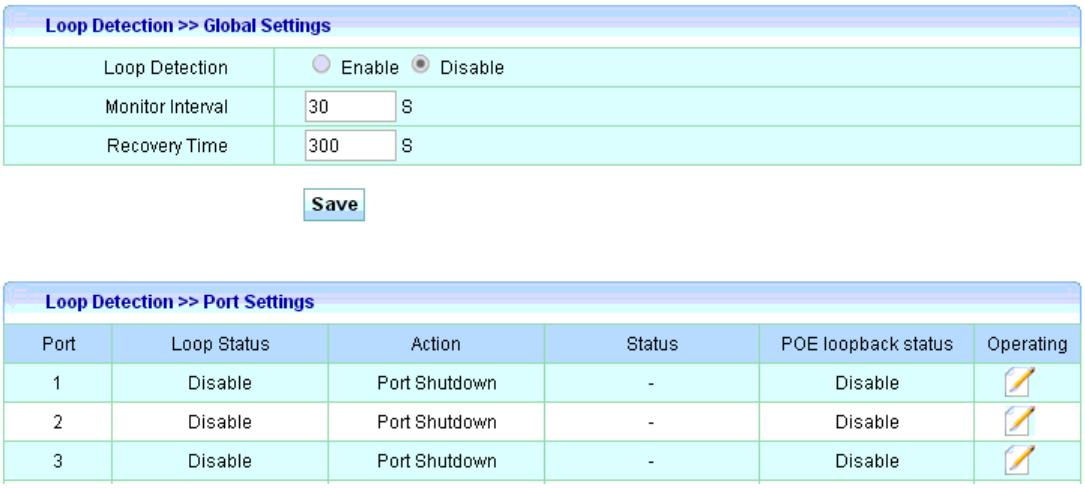
Network > STP > STP Port Information

Item	Description
Port	Designated port number.
Status	Displays whether the port is enabled or disabled.
Destination Root MAC	MAC address of the designated root port.
Destination Bridge MAC	MAC address of the designated bridge.

4.2.13. Loop Detection

Use this section to enable/disable and configure network routing loop detection.

To view the Loop Detection menu, navigate to Network > Loop Detection.



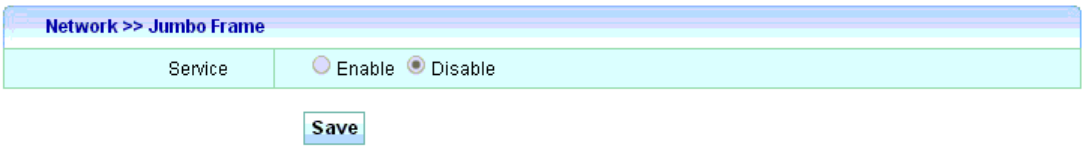
Network > Loop Detection

Item	Description
Loop Detection >> Global Settings	
Loop Detection	Displays whether loop detection is enabled or disabled.
Monitor Interval	Specifies how often a test packet is sent on a port.
Recovery Time	Number of seconds the device will wait before automatically re-enabling ports that were disabled due to a loop detection.
Save	Click **Save** to save the values and update the screen.
Loop Detection >> Port Settings	
Port	Designated port number.
Loop Status	Displays whether loop is enabled or disabled.
Action	Displays the action the port will take in case of loop detection.
Status	Displays current port status.
PoE loopback status	Displays whether PoE loopback status is enabled or disabled.
Operating	Click to configure loop detection settings by entering the following data: • Loop status (enable, disable) • Action (port blocking, port shutdown) • PoE loopback status (enable, disable)

4.2.14. Jumbo Frame

Use this section to enable jumbo frames.

To view the Jumbo Frame menu, navigate to Network > Jumbo Frame.



Network > Jumbo Frame

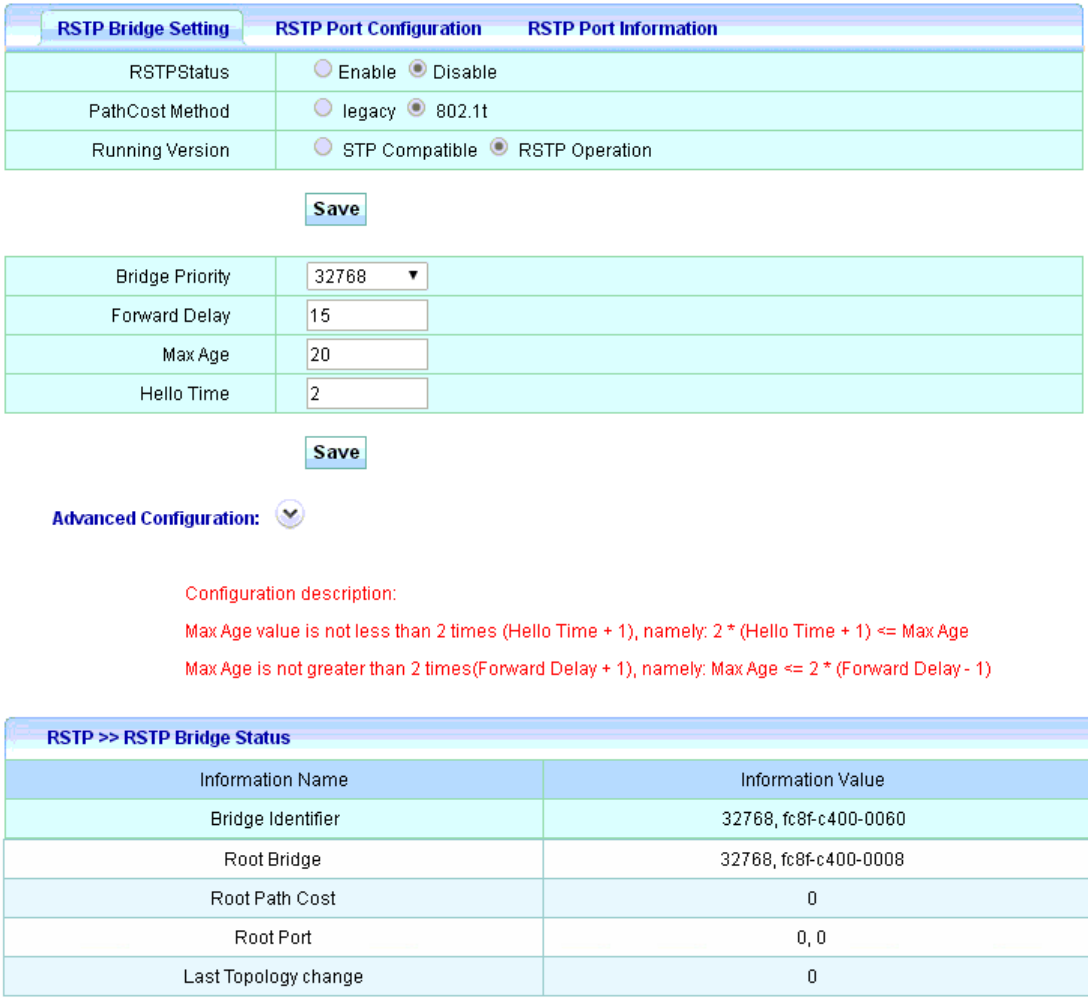
Item	Description
Service	Enable/disable jumbo frames.
Save	Click **Save** to save the values and update the screen.

4.2.15. RSTP

Use this section to configure Rapid Spanning Tree Protocol (RSTP).

RSTP Bridge Setting

To view the RSTP Bridge Setting menu, navigate to Network > RSTP > RSTP Bridge Setting.



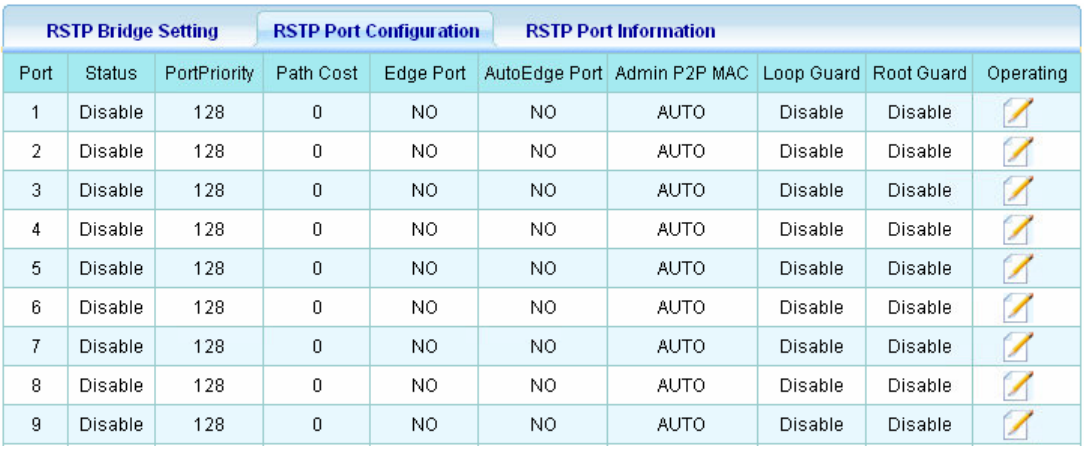
Network > RSTP > RSTP Bridge Setting

Item	Description
RSTP Status	Enable/disable RSTP.
PathCost Method	Select preferred pathcost method, legacy or 802.11.
Running Version	Select running version: • STP Compatible: Compatible with Spanning Tree Protocol • RSTP Operation: Rapid Spanning Tree Protocol
Bridge Priority	Select which bridge is elected as the root bridge and which bridge is elected as the root bridge when the initial root bridge fails.

Item	Description
Forward Delay	The amount of time a bridge remains in a listening and learning state before forwarding packets.
Max Age	The amount of time a bridge waits before implementing a topological change.
Hello Time	Time between each bridge protocol data unit (BPDU) sent on a port.
RSTP >> RSTP Bridge Status	
Information Name	
Bridge Identifier	Identification of the elected root bridge.
Root Bridge	Bridge on each LAN that provides the minimum root path cost.
Root Path Cost	The path cost to the designated root for the CST. Traffic from a connected device to the root bridge takes the least-cost path to the bridge. If the value is 0, the cost is automatically calculated based on port speed.
Root Port	The port with the lowest path cost to the bridge.
Last Topology/ Change	Time of the last network topology change.

RSTP Port Configuration

To view the RSTP Port Configuration menu, navigate to Network > RSTP > RSTP Port Configuration.

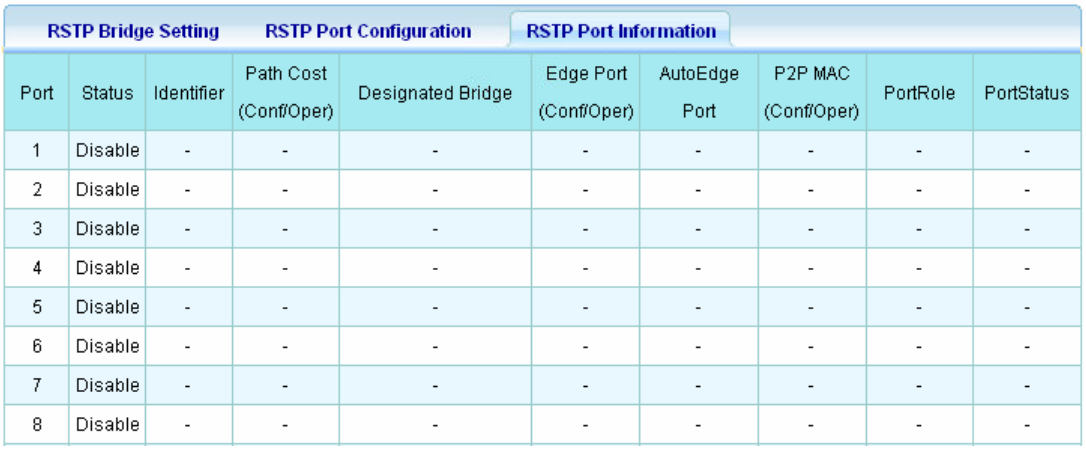


Network > RSTP > RSTP Port Configuration

Item	Description
Port	Designated port number.
Status	Displays whether port is enabled or disabled.
Port Priority	The priority for the port within the Common Spanning Tree (CST). This value is used in determining which port on a switch becomes the root port when two ports have the same least-cost path to the root. The port with the lower priority value becomes the root port. If the priority values are the same, the port with the lower interface index becomes the root port.
Path Cost	The path cost to the designated root for the CST. Traffic from a connected device to the root bridge takes the least-cost path to the bridge. If the value is 0, the cost is automatically calculated based on port speed.
Edge Port	Displays whether or not the port is an edge port (port of a bridge that connect to workstations or computers).
AutoEdge Port	Displays whether or not the port is an auto-edge port (the port will look for BPDUs for 3 seconds; if there are none it begins forwarding packets).
Admin P2P MAC	Displays Point-to-Point port configuration.
Loop Guard	Improves the stability of Layer 2 networks by preventing bridging loops.
Root Guard	Prevents switches connected on ports configured as access ports, from becoming the root switch.
Operating	Click to configure RSTP port configuration settings by entering the following data: • Status (enable, disable) • Port priority (0-240) • Path cost • Edge port (yes, no) • Auto edge port (yes, no) • Admin P2P MAC (auto, true, false) • Loop guard (enable, disable) • Root guard (enable, disable)

RSTP Port Information

To view the RSTP Port Information menu, navigate to Network > RSTP > RSTP Port Information.



RSTP Bridge Setting | RSTP Port Configuration | RSTP Port Information

Port	Status	Identifier	Path Cost (Conf/Oper)	Designated Bridge	Edge Port (Conf/Oper)	AutoEdge Port	P2P MAC (Conf/Oper)	PortRole	PortStatus
1	Disable	-	-	-	-	-	-	-	-
2	Disable	-	-	-	-	-	-	-	-
3	Disable	-	-	-	-	-	-	-	-
4	Disable	-	-	-	-	-	-	-	-
5	Disable	-	-	-	-	-	-	-	-
6	Disable	-	-	-	-	-	-	-	-
7	Disable	-	-	-	-	-	-	-	-
8	Disable	-	-	-	-	-	-	-	-

Network > RSTP > RSTP Port Information

Item	Description
Port	Designated port number.
Status	Displays whether port is enabled or disabled.
Identifier	Unique value that is automatically generated based on the bridge priority value and the base MAC address of the bridge.
Path Cost	The path cost to the designated root for the CST. Traffic from a connected device to the root bridge takes the least-cost path to the bridge. If the value is 0, the cost is automatically calculated based on port speed.
Designated Bridge	Bridge on each LAN that provides the minimum root path cost.
Edge Port	Displays whether or not the port is an edge port (port of a bridge that connect to workstations or computers).
AutoEdge Port	Displays whether or not the port is an auto-edge port (the port will look for BPDUs for 3 seconds; if there are none it begins forwarding packets).
Admin P2P MAC	Displays Point-to-Point port configuration.

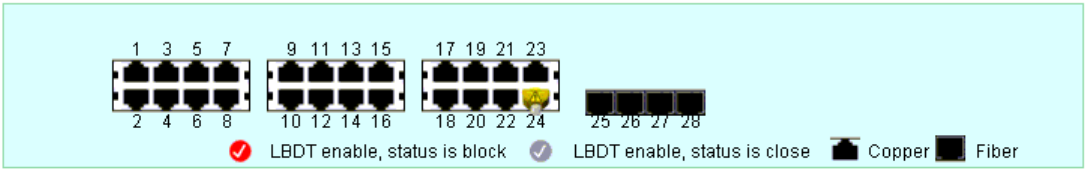
Item	Description
PortRole	The role of the port within the MST, which is one of the following: • Root: A port on the non-root bridge that has the least-cost path to the root bridge. • Designated: A port that has the least-cost path to the root bridge on its segment. • Alternate: A blocked port that has an alternate path to the root bridge. • Backup: A blocked port that has a redundant path to the same network segment as another port on the bridge. • Master: The port on a bridge within an MST instance that links the MST instance to other STP regions. • Disabled: The port is administratively disabled, and is not part of the spanning tree.
PortStatus	The current status of the port, which is one of the following: • Blocking: The port discards user traffic and receives, but does not send, BPDUs. During the election process, all ports are in the blocking state. The port is blocked to prevent network loops. • Listening: The port sends and receives BPDUs and evaluates information to provide a loop-free topology. This state occurs during network convergence and is the first state in transitioning to the forwarding state. • Learning: The port learns the MAC addresses of frames it receives and begins to populate the MAC address table. This state occurs during network convergence and is the second state in transitioning to the forwarding state. • Forwarding: The port sends and receives user traffic. • Disabled: The port is administratively disabled and is not part of the spanning tree.

4.3. Port Configuration

Use this section to configure switch physical port settings.

4.3.1. Port Configuration

To view the Port Configuration menu, navigate to Port Configuration > Port Configuration.



Port Configuration >> Port Configuration

PortID	Management	Auto Negotiation	Link	Real Speed	Manage Speed	Maximum Speed	Duplex	Flow Control	Description	Operating
1	Enable	Enable	Down	0M	Auto	1000M	Full	Open		
2	Enable	Enable	Down	0M	Auto	1000M	Full	Open		
3	Enable	Enable	Down	0M	Auto	1000M	Full	Open		
4	Enable	Enable	Down	0M	Auto	1000M	Full	Open		
5	Enable	Enable	Down	0M	Auto	1000M	Full	Open		

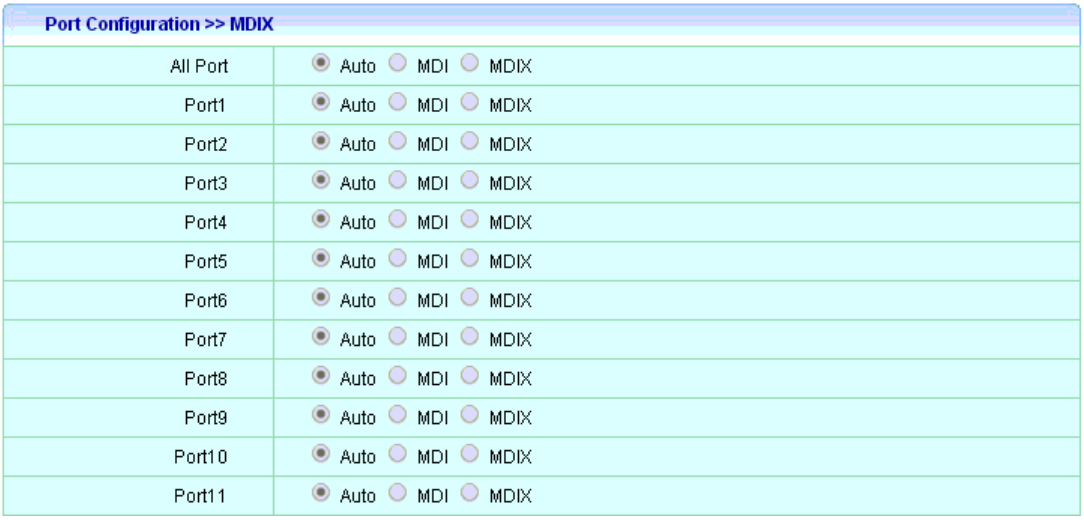
Port Configuration > Port Configuration

Item	Description
PortID	Identifier of switch physical port.
Management	Displays whether port management is enabled or disabled.
Link	Displays whether port is uplink or downlink.
Real Speed	Displays the actual port speed.
Manage Speed	Displays the speed management mode: Auto, Full, half.
Maximum Speed	Displays current maximum speed.
Duplex	Displays current duplex setting (half duplex or full duplex).
Flow Control	Displays current flow control setting.
Description	Displays user defined port description.
Operating	Click to configure port configuration settings by entering the following data: • Status (enable, disable) • Auto negotiation (enable, disable) • Flow control (open, close) • Description

4.3.2. MDIX Configuration

Use this section to configure MDIX settings. Each port can be designated as an MDI port or MDIX port, or have automatic MDI/MDIX detection enabled.

To view the MDIX Configuration menu, navigate to Port Configuration > MDIX Configuration.



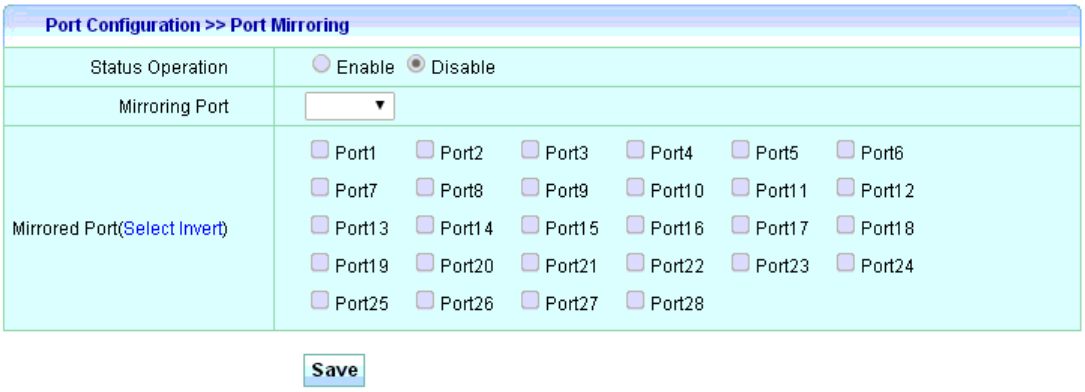
Port Configuration > MDIX Configuration

Item	Description
Auto	Set automatic MDI/MDIX detection.
MDI	Designate the port as an MDI port.
MDIX	Designate the port as an MDIX port.

4.3.3. Port Mirroring

Port mirroring selects the network traffic for analysis by a network analyzer. This is done for specific ports of the switch. As such, many switch ports are configured as source ports and one switch port is configured as a destination port.

To view the Port Mirroring menu, navigate to Port Configuration > Port Mirroring.



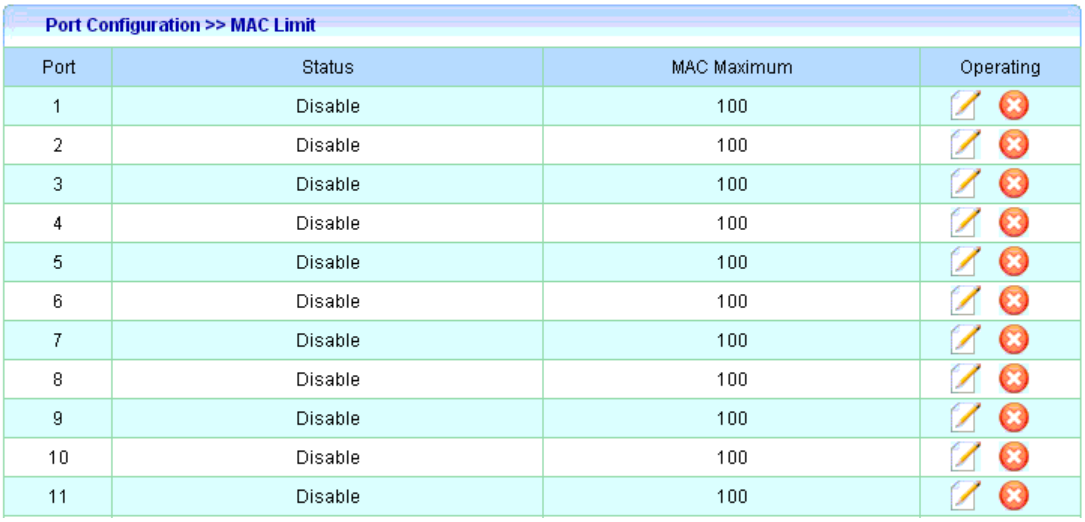
Port Configuration > Port Mirroring

Item	Description
Status Operation	Enable/disable port mirroring.
Mirroring Port	Select the mirror destination port.
Mirrored Port	The ports or configured to mirror traffic to the destination. Multiple source ports can be configured. Click **Select Invert** to invert current selection.
Save	Click **Save** to save the values and update the screen.

4.3.4. MAC Limit

Use this section configure MAC limit settings, to protect against flooding of the Ethernet switching table.

To view the MAC Limit menu, navigate to Port Configuration > MAC Limit.



Port Configuration > MAC Limit

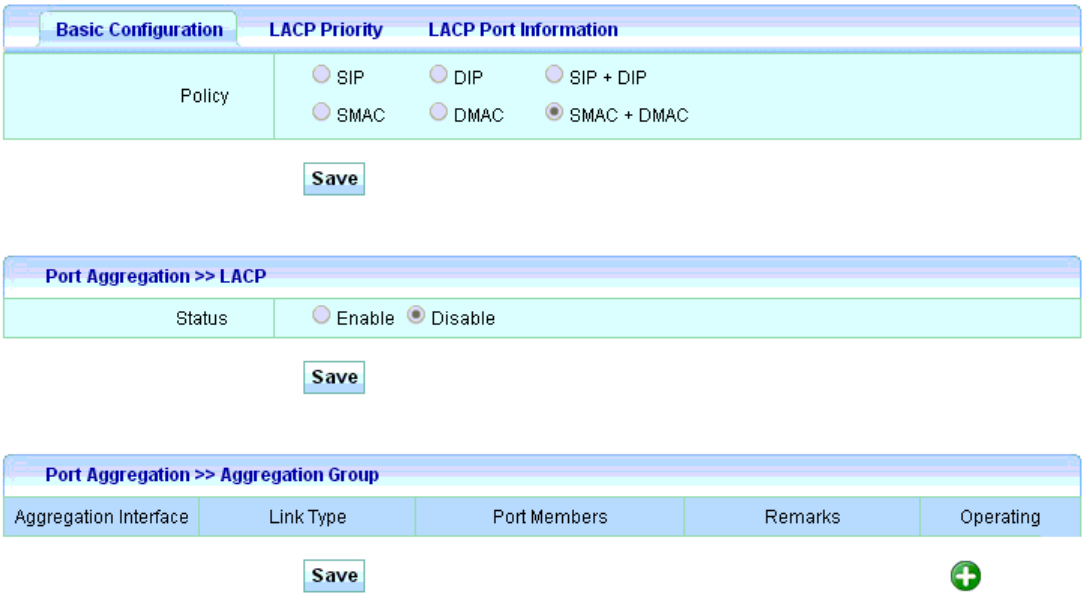
Item	Description
Port	Designated port number.
Status	Displays whether MAC limit is enabled or disabled on port.
MAC Maximum	Maximum number of secure MAC addresses for the interface.
Operating	Click to configure MAC limit settings by entering the following data: • Status (enable, disable) • MAC maximum (1-100)

4.3.5. Port Aggregation

Use this option to aggregate multiple Ethernet ports together to form a logical port. This feature supports static allocation and Link Aggregation Control Protocol (LACP).

Basic Configuration

To view the Basic Configuration menu, navigate to Port Configuration > Port Aggregation > Basic Configuration.



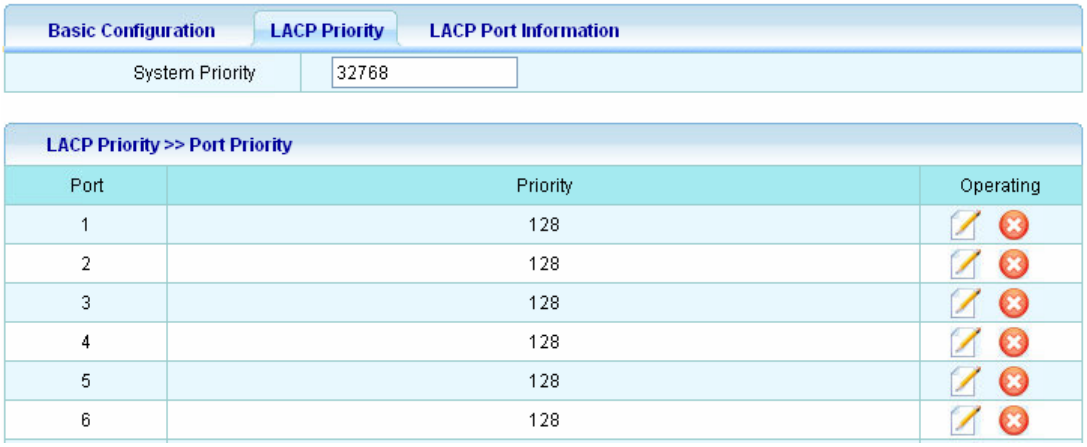
Port Configuration > Port Aggregation > Basic Configuration

Item	Description
Basic Configuration	
Policy	Select an LACP policy.
Save	Click **Save** to save the values and update the screen.
Port Aggregation >> LACP	
Status	Enable/disable LACP.
Save	Click **Save** to save the values and update the screen.
Port Aggregation >> Aggregation Group	
Aggregation Interface	Displays the aggregate identifier port.

Item	Description
Link Type	The type of port channel: • Dynamic: Uses LACP Protocol Data Units (PDUs) to exchange information with the link partners to help maintain the link state. To utilize Dynamic link aggregation on this port channel, the link partner must also support LACP. • Static: Does not require a partner system to be able to aggregate its member ports. When a port is added to a port channel as a static member, it neither transmits nor receives LACP PDUs.
Port Members	The ports that are members of a port channel.
Remarks	User added comments.
Operating	Click to add new aggregation groups by entering the following data: • Aggregation interface number • Link type (static, dynamic) • Port number • Remarks
Save	Click **Save** to save the values and update the screen.

LACP Priority

To view the LACP Priority menu, navigate to Port Configuration > Port Aggregation > LACP Priority.



Port Configuration > Port Aggregation > LACP Priority

Item	Description
Port	Designated port number.
Priority	The priority for the port within the MSTI. This value is used in determining which port on a switch becomes the root port when two ports have the same least-cost path to the root. The port with the lower priority value becomes the root port. If the priority values are the same, the port with the lower interface index becomes the root port.
Operating	Click to configure LACP priority settings by entering the following data: • Priority (0-255)

LACP Port Information

This window displays LACP port information.

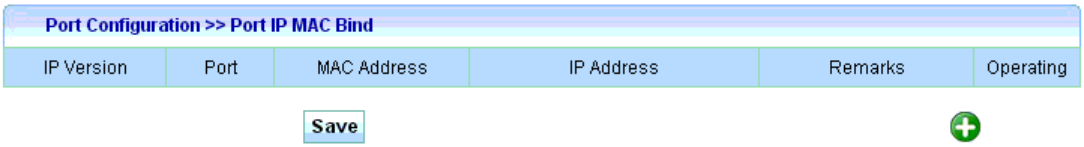
To view the LACP Port Information menu, navigate to Port Configuration > Port Aggregation > LACP Port Information.

Port Configuration > Port Aggregation > LACP Port Information

4.3.6. Port-IP-MAC Binding

Use this section to configure IP-MAC-Port binding to improve network security.

To view the Port-IP-MAC Binding menu, navigate to Port Configuration > Port-IP-MAC Binding.



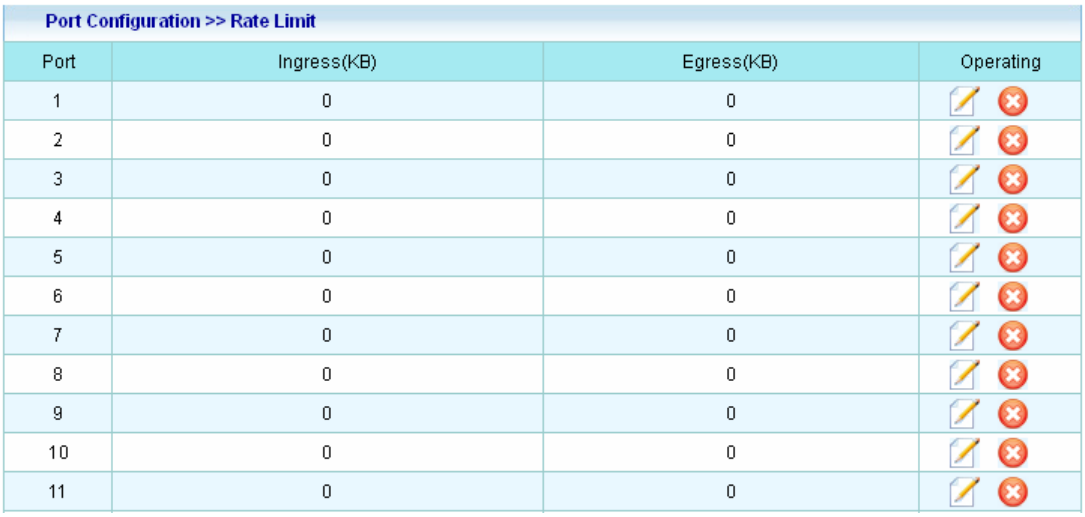
Port Configuration > Port-IP-MAC Binding

Item	Description
IP Version	Displays the IP version (IPv4 or IPv6).
Port	Designated port number.
MAC Address	MAC address of the designated port.
IP Address	IP address of the designated port.
Remarks	User added comments.
Operating	Click to add new Port-IP-MAC binding entries by entering the following data: • IP version (IPv4, IPv6) • IP address • MAC address • Remarks
Save	Click **Save** to save the values and update the screen.

4.3.7. Rate Limit

This page allows you to set ingress port monitoring.

To view the Rate Limit menu, navigate to Port Configuration > Rate Limit.



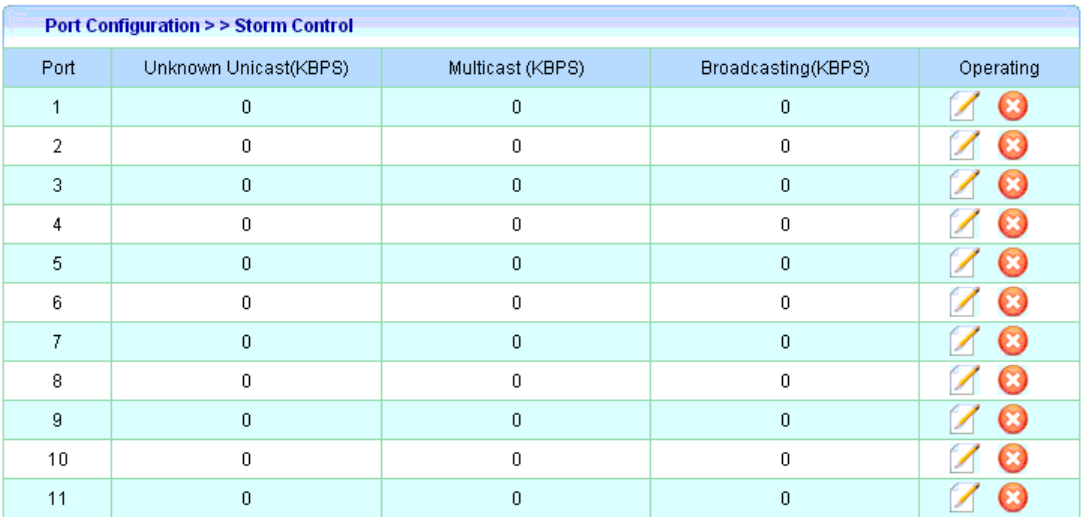
Port Configuration > Rate Limit

Item	Description
Port	Designated port number.
Ingress (KB)	The upper limit on how much traffic can enter a port.
Egress (KB)	The upper limit on how much traffic can exit a port.
Operating	Click to configure port limit settings by entering the following data: • Ingress limit (KB) • Egress limit (KB)

4.3.8. Storm Control

Use this section to set ingress port monitoring.

To view the Storm Control menu, navigate to Port Configuration > Storm Control.



Port Configuration > Storm Control

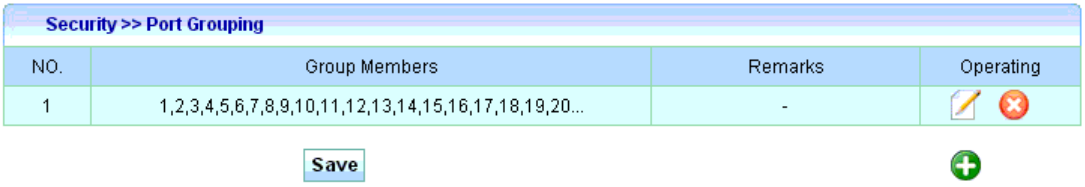
Item	Description
Port	Designated port number.
Unknown Unicast (KBPS)	Traffic sent by unknown unicast.
Multicast (KBPS)	Traffic sent by multicast.
Broadcasting (KBPS)	Traffic sent by broadcast.
Operating	Click to configure storm control settings by setting traffic limits: • Unknown unicast limit (KB) • Multicast limit (KB) • Broadcasting limit (KB)

4.4. Security

Port security can set port isolation and specific behavior.

4.4.1. Port Grouping

To view the Port Grouping menu, navigate to Security > Port Grouping.



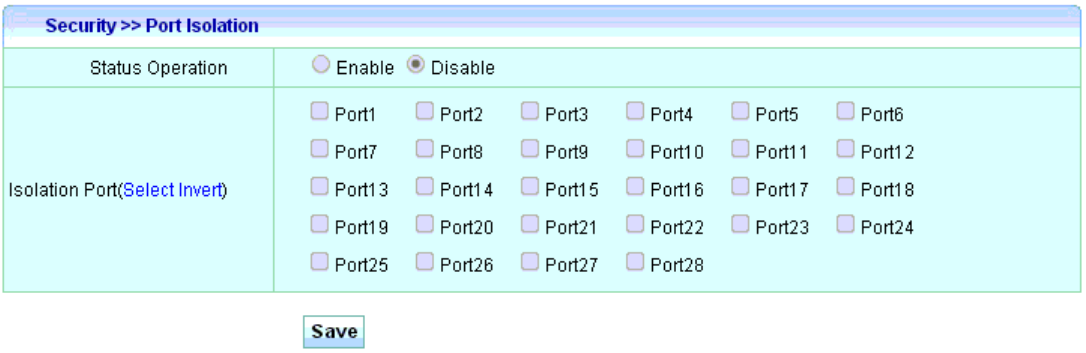
Security > Port Grouping

Item	Description
No.	Designated port number.
Group members	Ports in the group.
Remarks	User added comments.
Operating	Edit existing port groups by entering the following data: • Group members (select ports) • Remarks Click to add new port groups by entering the following data: • Group members (select ports) • Remarks

4.4.2. Port Isolation

Use this section to isolate switch ports so Layer 2 network traffic will not be forwarded between them.

To view the Port Isolation menu, navigate to Security > Port Isolation.



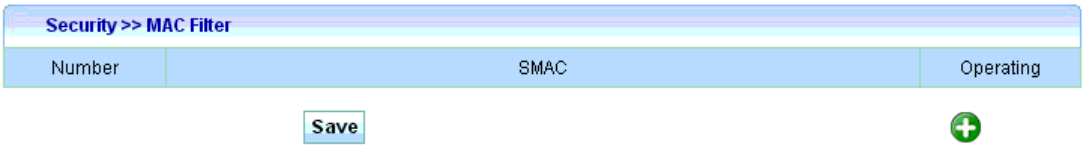
Security > Port Isolation

Item	Description
Status Operation	Enable/disable port isolation.
Isolation Port	Select ports to isolate. Click **Select Invert** to invert current selection.
Save	Click **Save** to save the values and update the screen.

4.4.3. MAC Filter

Use this section to create a list of MAC addresses which are permitted or denied network access.

To view the MAC Filter menu, navigate to Security > MAC Filter.



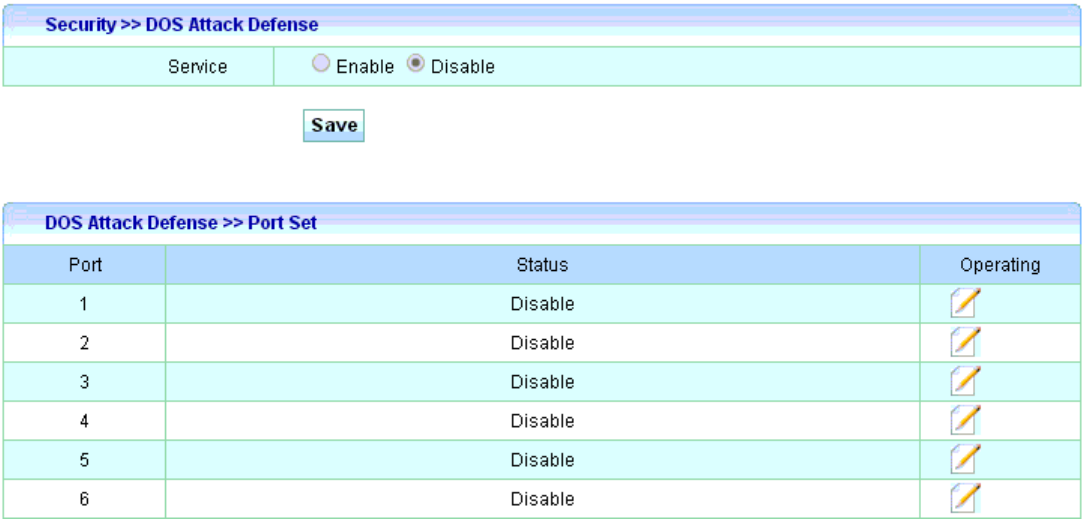
Security > MAC Filter

Item	Description
Number	MAC address to mask.
SMAC	Smac MAC Address Changer, used to mask a MAC address.
Operating	Click to add MAC filter entries by entering the following data: • SMAC

4.4.4. DoS Defense

Use this section to enable and configure Denial of Service defense on switch ports.

To view the DoS Defense menu, navigate to Security > DoS Defense.



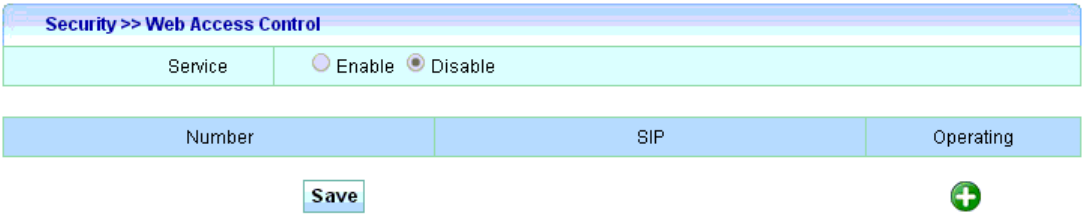
Security > DoS Defense

Item	Description
Security >> DoS Defense	
Service	Enable/disable.
Save	Click **Save** to save the values and update the screen.
Security >> Port Set	
Port	Designated port number.
Status	Displays whether DoS defense is enabled or disabled.
Operating	Click to configure DoS defense settings for each port by entering the following data: • Status (enable, disable)
Save	Click **Save** to save the values and update the screen.

4.4.5. Web Access Control

Use this section to enable and configure web access control.

To view the Web Access Control menu, navigate to Security > Web Access Control.



Security > Web Access Control

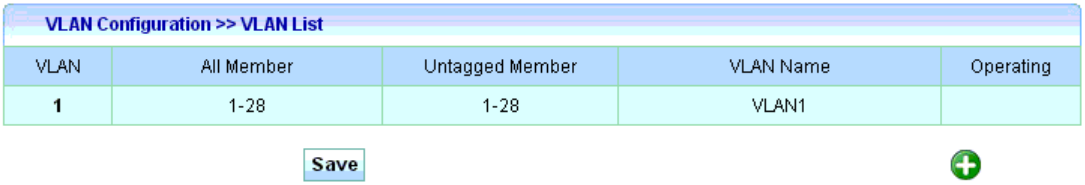
Item	Description
Service	Enable/disable web access control.
Number	Designated port number.
SIP	Session Initiation Protocol command.
Operating	Click to configure web access control settings by entering the following data: • SIP

4.5. VLAN Configuration

Use this section to configure IEEE 802.1Q settings carrying Virtual Local Area Network (VLAN) traffic.

4.5.1. 802.1Q VLAN

To view the 802.1Q VLAN menu, navigate to VLAN Configuration > 802.1Q VLAN.



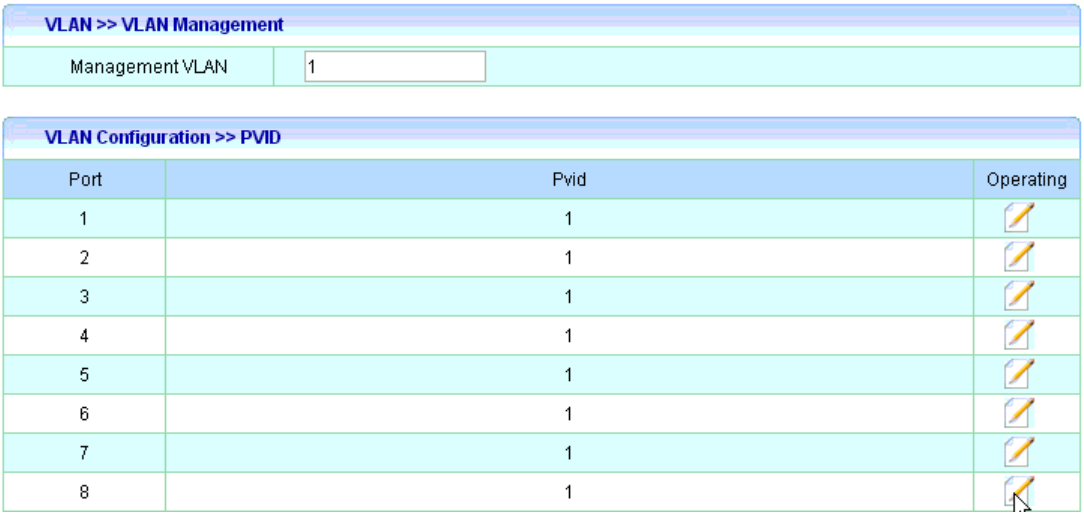
VLAN Configuration > 802.1Q VLAN

Item	Description
VLAN	VLAN number.
All Member	Number of members in the VLAN.
Untagged Member	Number of untagged members in the VLAN.
VLAN Name	Name of the VLAN on the network.
Operating	Click to configure 802.1Q VLAN settings by entering the following data: • VLAN ID • VLAN group member tag settings (none, tagged, untagged) • VLAN remarks name

4.5.2. VLAN Management

Use this section to manage VLAN ID the selected ports.

To view the VLAN Management menu, navigate to VLAN Configuration > VLAN Management.



VLAN Configuration > VLAN Management

Item	Description
Port	Designated port number.
PVID	Port VLAN ID.
Operating	Click to configure VLAN management settings for each port by entering the following data: • PVID

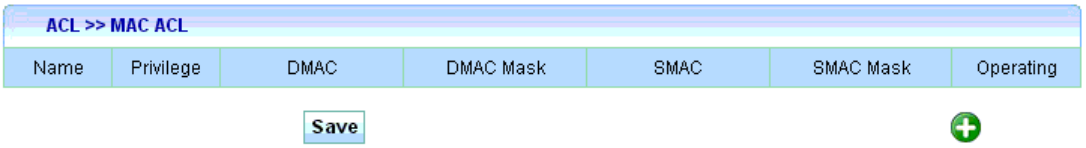
4.6. ACL

The ACL section can help limit network traffic and restrict network use by certain users or devices. The following section allows you to manage ACLs on the system and view summary information.

4.6.1. MAC ACL

Use this section to configure MAC Access Control Lists (ACL).

To view the MAC ACL menu, navigate to ACL > MAC ACL.



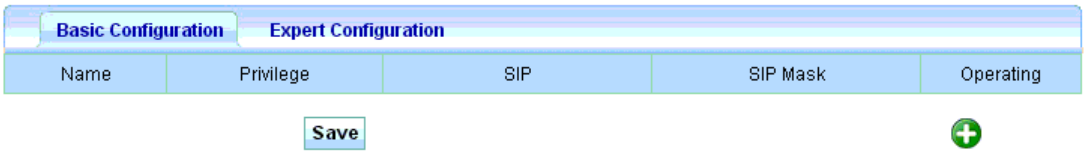
ACL > MAC ACL

Item	Description
Name	MAC Access Control List (ACL) name.
Privilege	Port access rights.
DMAC	MAC DA distributes traffic based on a packet's destination MAC address.
DMAC Mask	Enter the mask values of a MAC network to apply to the VLAN filter to the forwarding vector, effectively masking the destination MAC address.
SMAC	Smac MAC Address Changer, used to mask a MAC address.
SMAC Mask	Masked MAC address generated by SMAC.
Operating	Click to configure MAC ACL settings by entering the following data: • Name • Privilege (permit or deny) • DMAC Mask • SMAC • SMAC Mask

4.6.2. IP ACL

Use this section to configure IP Access Control Lists (ACL).

To view the IP ACL menu, navigate to ACL > IP ACL.



ACL > IP ACL

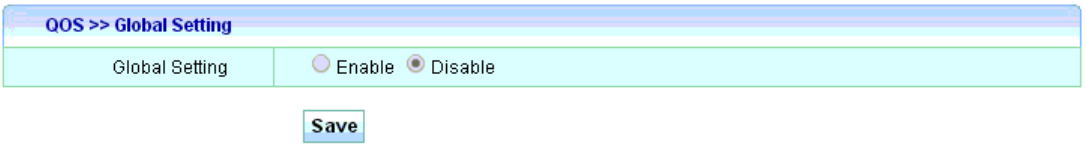
Item	Description
Name	MAC Access Control List (ACL) name.
Privilege	Port access rights.
SIP	Session Initiation Protocol command.
SIP Mask	IP address mask for SIP traffic.
Operating	Click to configure IP ACL settings by entering the following data: • Name • Privilege (permit, deny) • SIP • SIP Mask

4.7. QoS

Use this section to configure Quality of Service (QoS) settings.

4.7.1. Global Setting

To view the Global Setting menu, navigate to QoS > Global Setting.

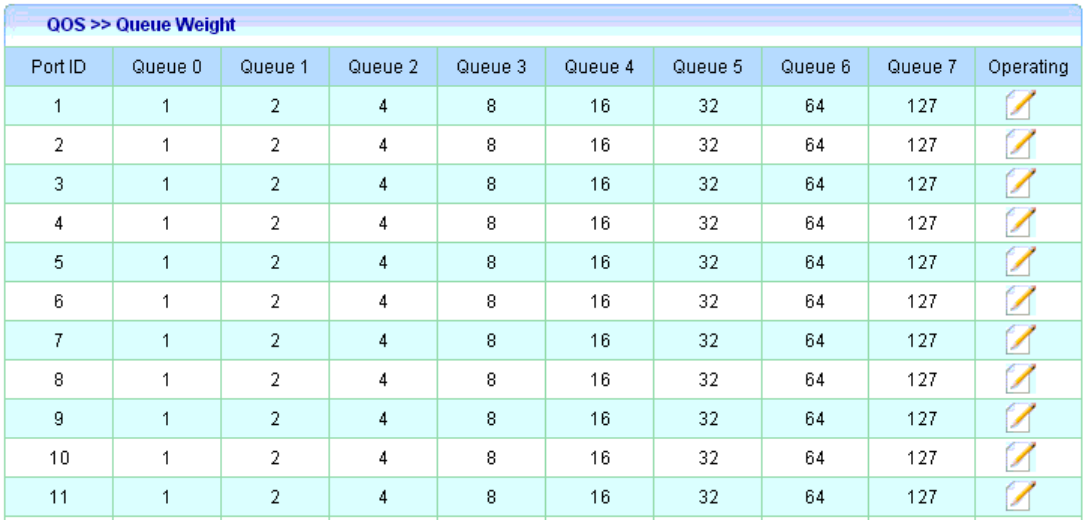


QoS > Global Setting

Item	Description
Global Setting	Enable/disable QoS.
Save	Click **Save** to save the values and update the screen.

4.7.2. Queue Weight

To view the Queue Weight menu, navigate to QoS > Queue Weight.



QOS >> Queue Weight

Port ID	Queue 0	Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7	Operating
1	1	2	4	8	16	32	64	127	
2	1	2	4	8	16	32	64	127	
3	1	2	4	8	16	32	64	127	
4	1	2	4	8	16	32	64	127	
5	1	2	4	8	16	32	64	127	
6	1	2	4	8	16	32	64	127	
7	1	2	4	8	16	32	64	127	
8	1	2	4	8	16	32	64	127	
9	1	2	4	8	16	32	64	127	
10	1	2	4	8	16	32	64	127	
11	1	2	4	8	16	32	64	127	

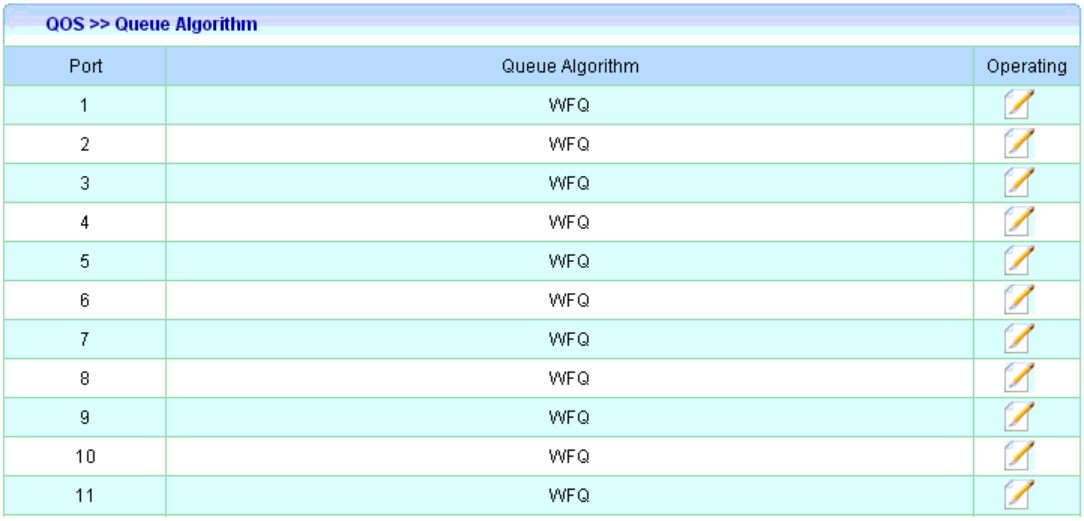
QoS > Queue Wait

Item	Description
Port ID	The port identifier, which is the physical address associated with the interface.
Queue 0-7	Queues used to store traffic until it can be processed or serialized.
Operating	Click to configure queue weight settings by entering the following data: • Queue 0-7 queue weight (0-127)

4.7.3. Queue Algorithm

Queue algorithms are used to regulate network traffic to optimize QoS.

To view the Queue Algorithm menu, navigate to QoS > Queue Algorithm.

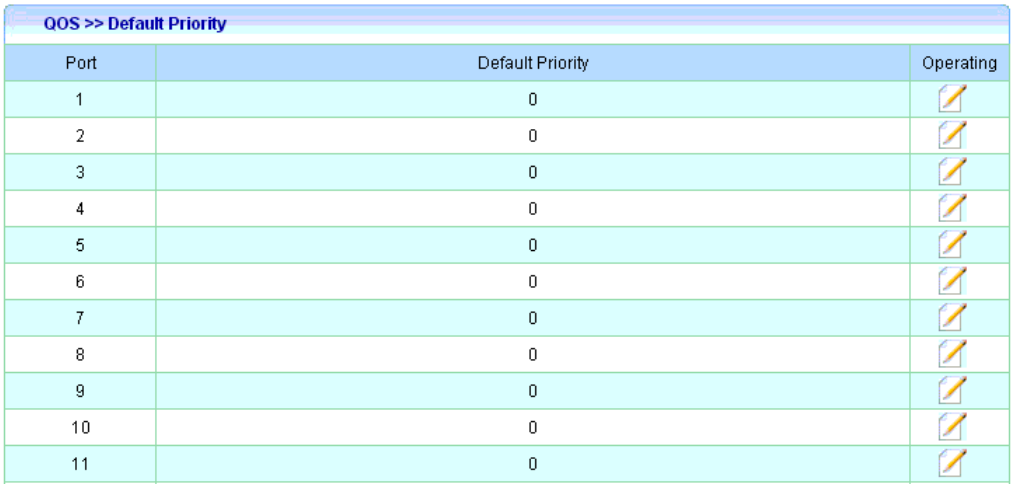


QoS > Queue Algorithm

Item	Description
Port	Designated port number.
Queue Algorithm	Displays current queue algorithm type.
Operating	Click to configure queue algorithm settings by entering the following data: • Queue algorithm (WFQ, WRR, WRR+SP)

4.7.4. Default Priority

To view the Default Priority menu, navigate to QoS > Default Priority.



QOS >> Default Priority

Port	Default Priority	Operating
1	0	
2	0	
3	0	
4	0	
5	0	
6	0	
7	0	
8	0	
9	0	
10	0	
11	0	

QoS > Default Priority

Item	Description
Port	Designated port number.
Default Priority	Priority automatically assigned by the default QoS rule.
Operating	Click to configure default priority settings by entering the following data: • Default priority (0-7)

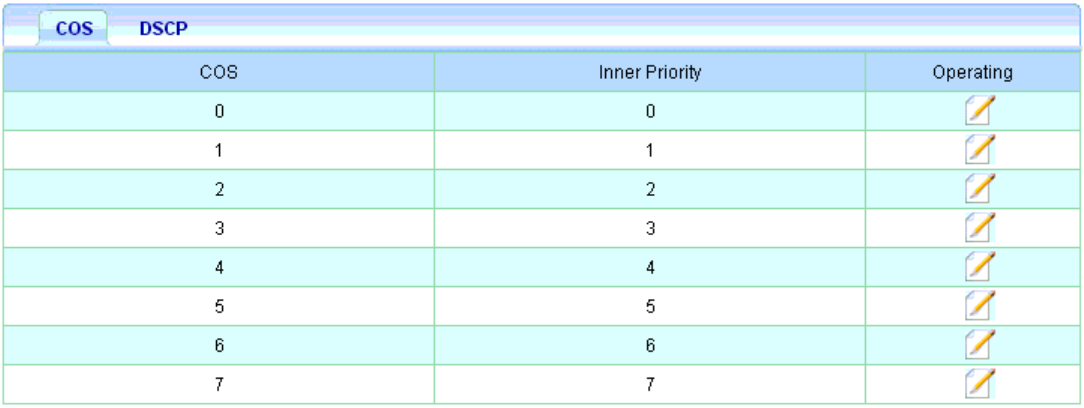
4.7.5. Priority Mapping

Use this section to view or change which internal traffic classes are mapped to the 802.1p priority class values in Ethernet frames the device receives.

CoS

Use this section to configure Class of Service settings.

To view the CoS menu, navigate to QoS > Priority Mapping > CoS.



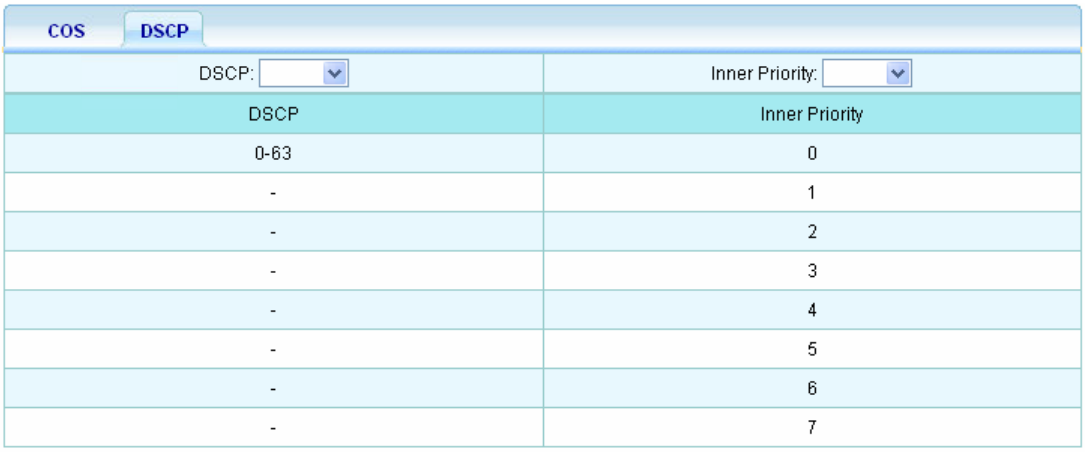
QoS > Priority Mapping > CoS

Item	Description
CoS	Class of service traffic profile.
Inner Priority	802.1p priority value (0-7).
Operating	Click to configure CoS settings by entering the following data for each CoS: • Inner priority (0-7)

DSCP

Differentiated Services Code Point (DSCP) enables different levels of service to be assigned to network traffic.

To view the DSCP menu, navigate to QoS > Priority Mapping > DSCP.



QoS > Priority Mapping > DSCP

Item	Description
DSCP	Enter DSCP code.
Inner Priority	Enter 802.1p priority value (0-7).

4.7.6. QoS Trust

Use this section to configure QoS trust settings. Individual ports can be assigned different QoS trust profiles.

To view the QoS Trust menu, navigate to QoS > Priority Mapping > QoS Trust.

QoS > Priority Mapping > QoS Trust

Item	Description
Port	Designated port number.
QoS Trust Mode	Select QoS Trust Mode: • CoS Only • DSCP Prior To The CoS • DSCP Only • Distrust

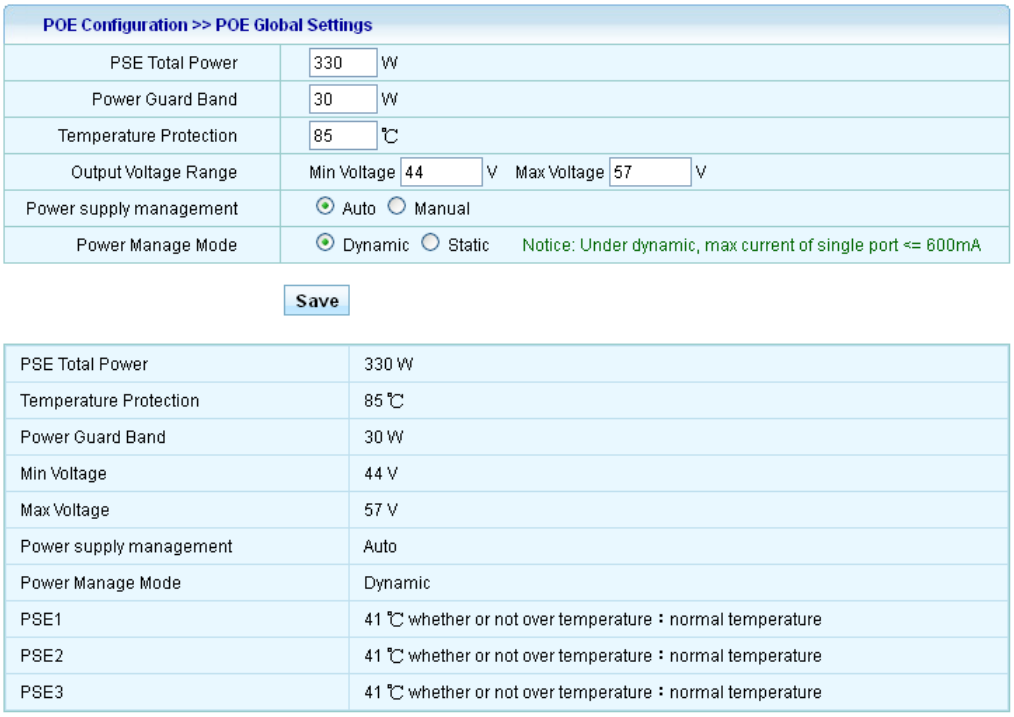
4.8. PoE Configuration

Use this section to configure PoE settings for the switch and its ports.

4.8.1. PoE Global Setting

Use this feature to check PoE Status and set maximum output power.

To view the PoE Global Setting menu, navigate to PoE Configuration > PoE Global Setting.



PoE Configuration > PoE Global Setting

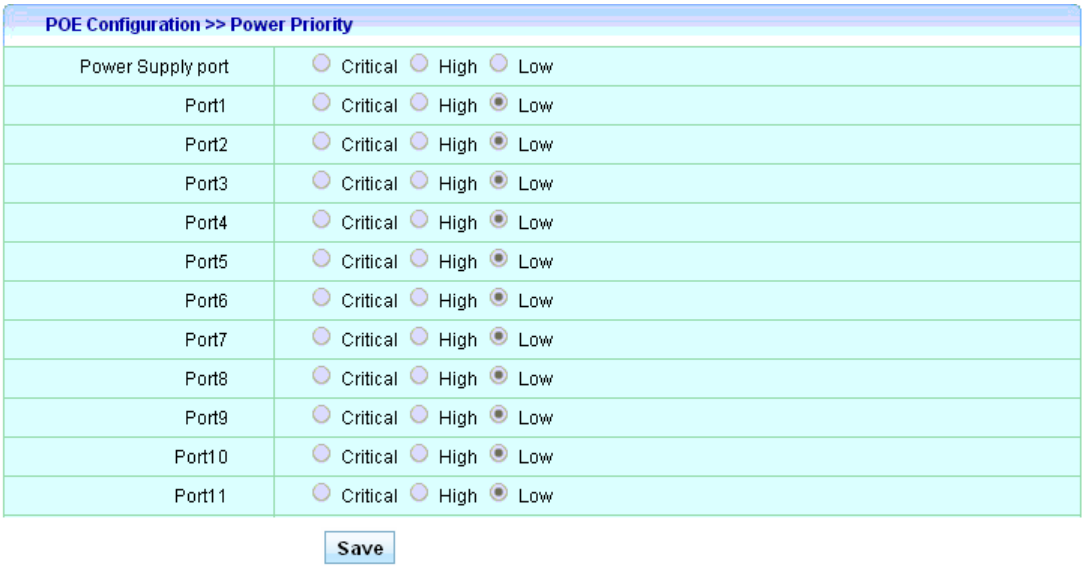
Item	Description
PoE Configuration >> PoE Global Settings	
PSE Total Power	Enter total PSE power.
Power Guard Band	Reserves a specified amount of power from the PoE power budget for the switch or the line card in case of a spike in PoE consumption.
Temperature Protection	Enter upper temperature limit which will trigger temperature protection activity.
Output Voltage Range	Configure PoE output voltage minimum and maximum.
Power supply management	Select if power supply is to be managed automatically or manually.
Power Manage Mode	Select if power supply management mode is to be dynamic or static.

Item	Description
Save	Click **Save** to save the values and update the screen.
PSE Total Power	Displays total PSE power.
Temperature Protection	Displays upper temperature limit which will trigger temperature protection activity.
Power Guard Band	Displays specified amount of power from the PoE power budget for the switch or the line card in case of a spike in PoE consumption.
Min Voltage	Displays the minimum voltage for PSEs.
Max Voltage	Displays the maximum voltage available for PSEs.
Power supply management	Displays the power supply management mode.
PSE1	Displays temperature of PSE1.
PSE2	Displays temperature of PSE2.
PSE3	Displays temperature of PSE3.
Refresh	Refresh the display.

4.8.2. Power Priority

Use this section to set the power supply priority of PoE ports. Individual ports can be assigned critical, high, or low power supply priority.

To view the Power Priority menu, navigate to PoE Configuration > Power Priority.

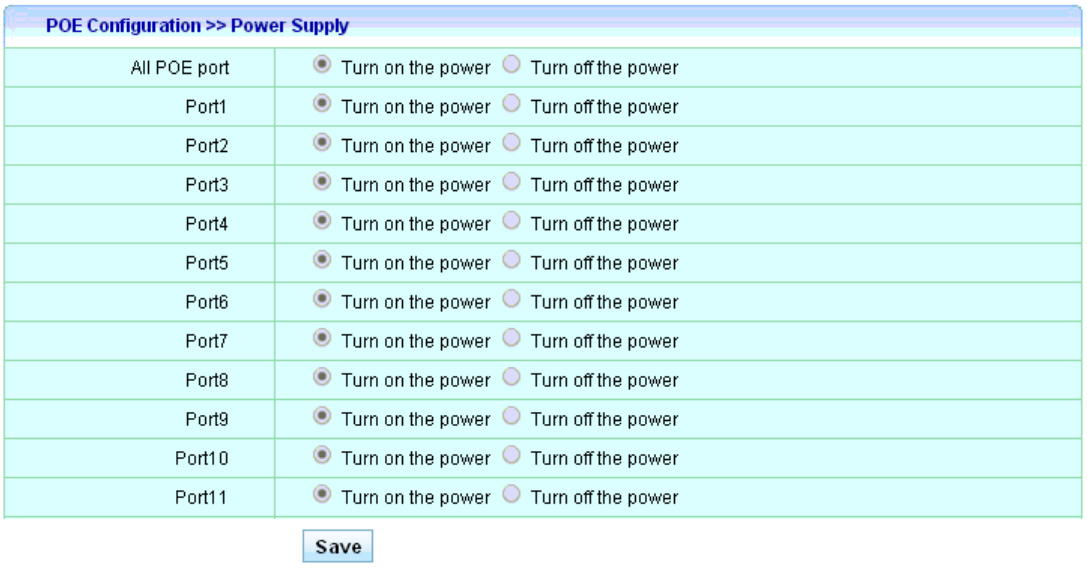


PoE Configuration > Power Priority

4.8.3. Power Supply

Use this section to manage power supply to PoE ports. Power to individual ports can be turned on or off.

To view the Power Supply menu, navigate to PoE Configuration > Power Supply.



PoE Configuration > Power Supply

4.8.4. PoE Timing Reboot

Use this section to configure PoE output power on/off schedules.

To view the PoE Timing Reboot menu, navigate to PoE Configuration > PoE Timing Reboot.

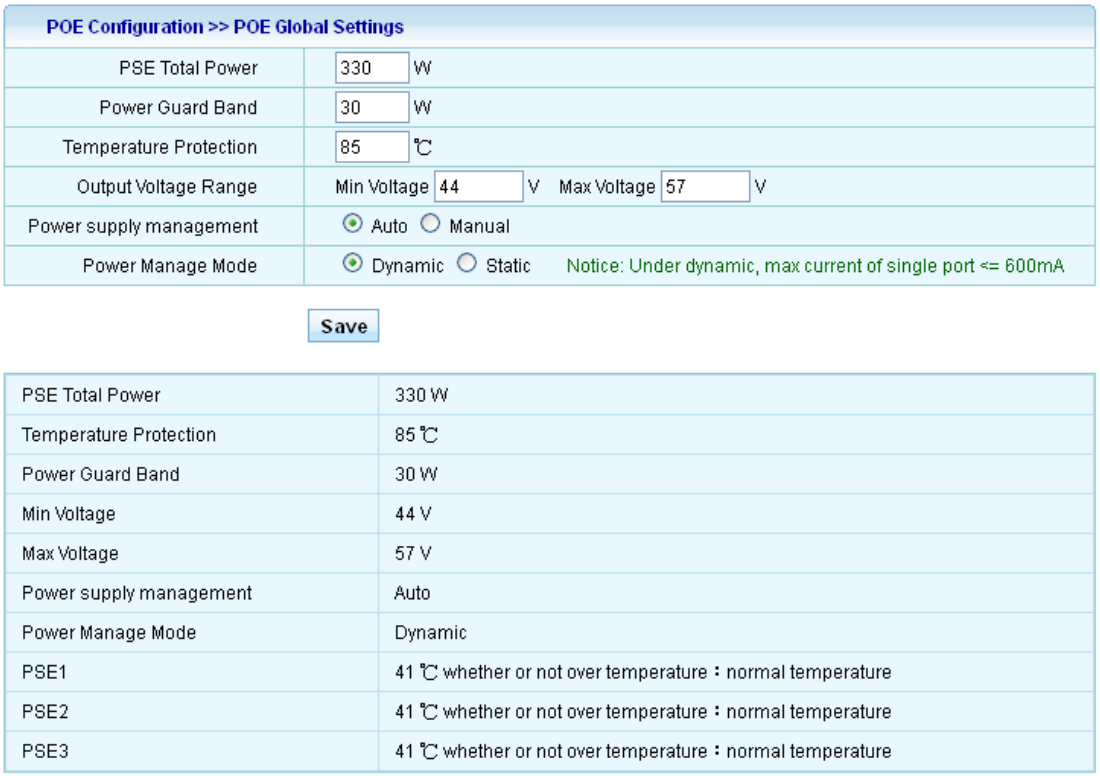
PoE Configuration > PoE Timing Reboot

Item	Description
No.	PoE output power on/off schedule number.
Status	Schedule status, active or inactive.
Time Of Duration	Duration for which power will be off.
Reboot Time	Time at which PoE will be rebooted.
Weeks	Day or days of the week on which the schedule will be activated.
Port	Designated port number.
Remarks	User added comments.
Operating	Click to configure PoE timing reboot settings by entering the following data: • No. (schedule number) • Status operation (enable, disable) • Reboot time (hours:minutes) • Weeks (day or days of the week on which the schedule will be activated) • All PoE port (select ports) • Remarks

4.8.5. Power Limitation

Use this section to configure PoE power limitation settings.

To view the Power Limitation menu, navigate to PoE Configuration > Power Limitation.



PoE Configuration > Power Limitation

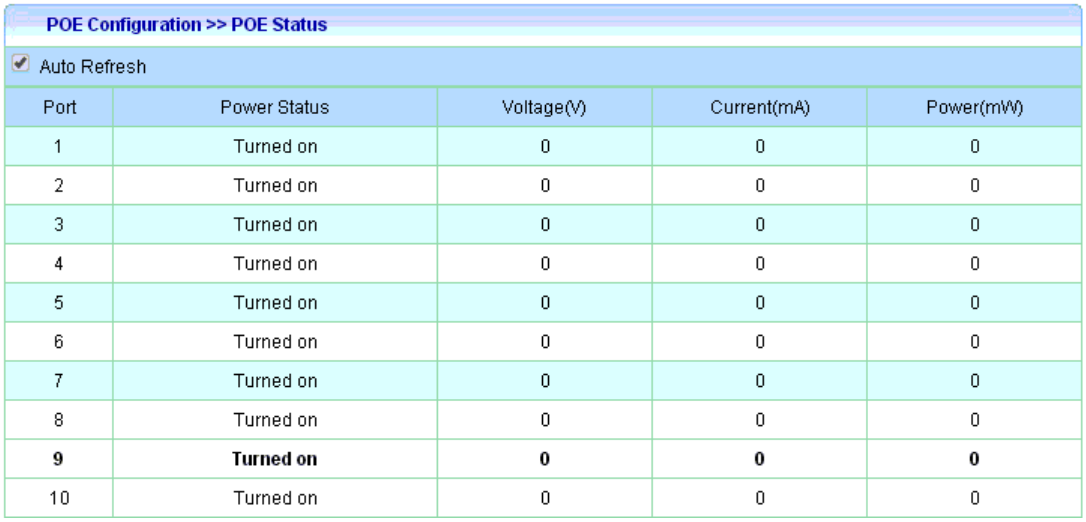
Item	Description
PSE Total Power	Enter total PSE power.
Power Guard Band	Reserves a specified amount of power from the PoE power budget for the switch or the line card in case of a spike in PoE consumption.
Temperature Protection	Enter upper temperature limit which will trigger temperature protection activity.
Output Voltage Range	Configure PoE output voltage minimum and maximum.
Power supply management	Select if power supply is to be managed automatically or manually.
Power Manage Mode	Select if power supply management mode is to be dynamic or static.
Save	Click **Save** to save the values and update the screen.
PSE Total Power	Displays total PSE power.
Temperature Protection	Displays upper temperature limit which will trigger temperature protection activity.

Item	Description
Power Guard Band	Displays specified amount of power from the PoE power budget for the switch or the line card in case of a spike in PoE consumption.
Min Voltage	Displays the minimum voltage for PSEs.
Max Voltage	Displays the maximum voltage available for PSEs.
Power supply management	Displays the power supply management mode.
PSE1	Displays temperature of PSE1.
PSE2	Displays temperature of PSE2.
PSE3	Displays temperature of PSE3.
Refresh	Refresh the display.

4.8.6. PoE Status

Use this section to monitor individual port PoE status.

To view the PoE Status menu, navigate to PoE Configuration > PoE Status.



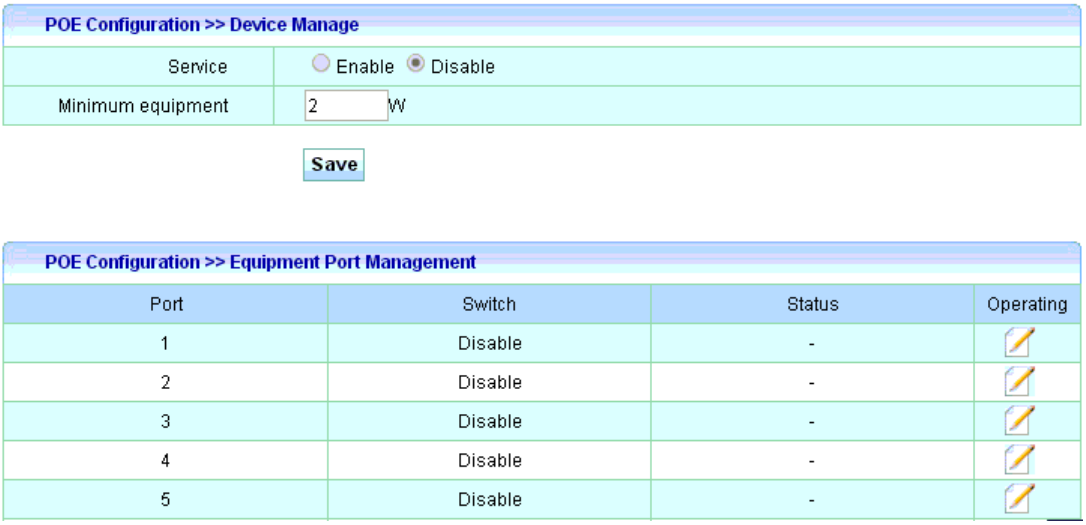
Port	Power Status	Voltage(V)	Current(mA)	Power(mW)
1	Turned on	0	0	0
2	Turned on	0	0	0
3	Turned on	0	0	0
4	Turned on	0	0	0
5	Turned on	0	0	0
6	Turned on	0	0	0
7	Turned on	0	0	0
8	Turned on	0	0	0
9	**Turned on**	**0**	**0**	**0**
10	Turned on	0	0	0

PoE Configuration > PoE Status

Item	Description
Auto Refresh	Automatically update data display periodically.
Port	Designated port number.
Power Status	Port PoE status (on or off).
Voltage (V)	Voltage drawn by port.
Current (mA)	Current drawn by port.
Power (mW)	Power drawn by port.

4.8.7. Device Manager

To view the Device Manager menu, navigate to PoE Configuration > Device Manager.



PoE Configuration > Device Manager

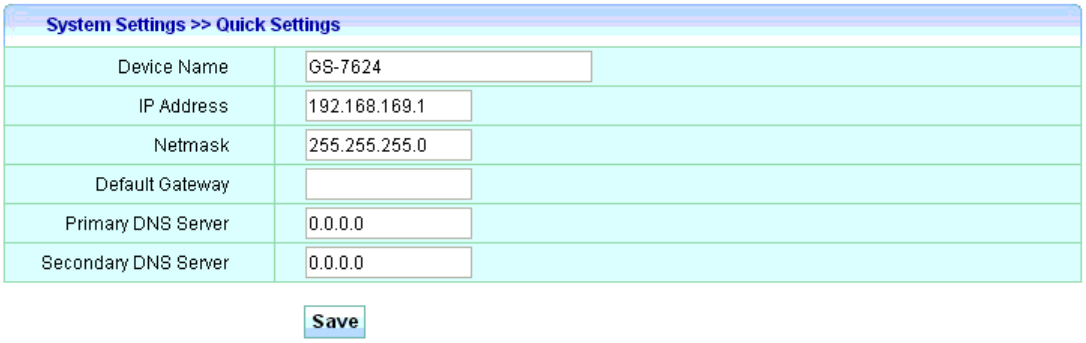
Item	Description
PoE Configuration >> Device Manager	
Service	Enable or disable device manager service.
Minimum equipment	Set a value in Watts for the minimum allowable consumption for power sourced equipment.
PoE Configuration >> Equipment Port Management	
Port	Designated port number.
Switch	Switch status (enable or disable).
Status	
Operating	Click to configure equipment port management settings by entering the following data: • Port switch (enable, disable)

4.9. System Settings

Use this section to configure switch network settings.

4.9.1. Quick Settings

To view the Quick Settings menu, navigate to System Settings > Quick Settings.

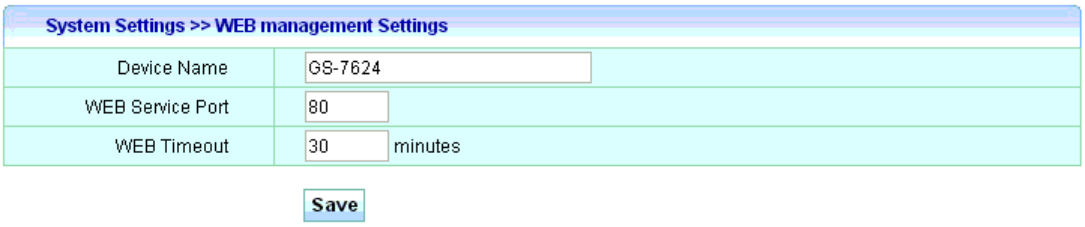


System Settings > Quick Setting

Item	Description
Device Name	Switch model number, configurable according to user preference.
IP Address	If static mode is enabled, enter IP address in this field.
Netmask	If static mode is enabled, enter subnet mask in this field.
Default Gateway	Enter a Gateway Address to be the address of a router that connects two different networks.
Primary DNS Server	Enter the IP addresses of a primary DNS server the client should use to resolve host names into IP addresses.
Secondary DNS Server	Enter the IP addresses of a secondary DNS server the client should use to resolve host names into IP addresses.
Save	Click **Save** to save the values and update the screen.

4.9.2. Web Management

To view the Web Management menu, navigate to System Settings > Web Management.



.

System Settings > Web Management

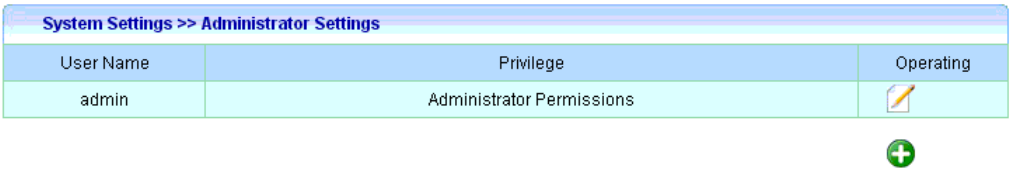
Item	Description
Device Name	Device model name.
WEB Service Port	Enter the port number used by the device for web services.
WEB Timeout	Enter the session time-out for an ASP application.
Save	Click **Save** to save the values and update the screen.

4.9.3. Administrator

Use this section to create and edit user accounts.

Administrator

To view the Administrator menu, navigate to System Settings > Administrator.

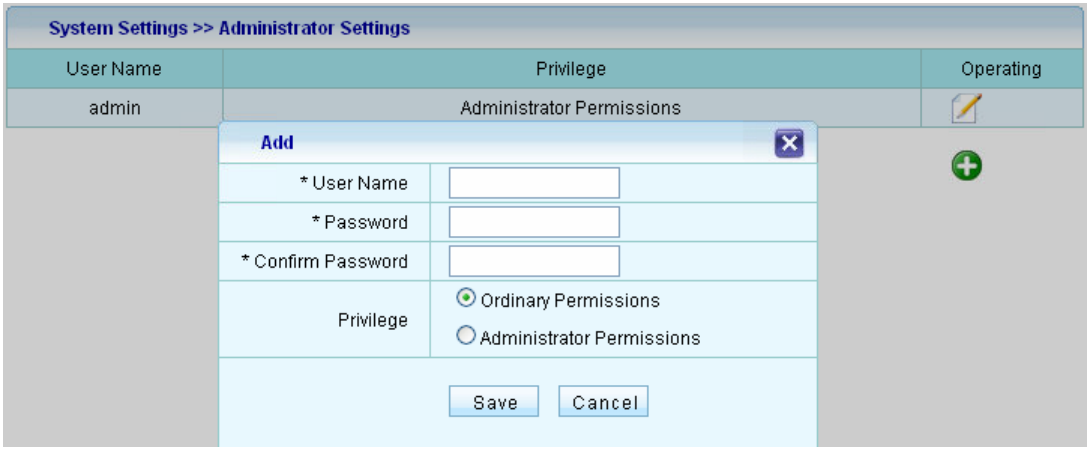


System Settings > Administrator

Item	Description
Username	Account username.
Privilege	Current level of account system privileges.
Operating	Click to add new user accounts and edit existing user accounts.

Use these settings to create a new account.

To view the Administrator menu, navigate to System Settings > Administrator.

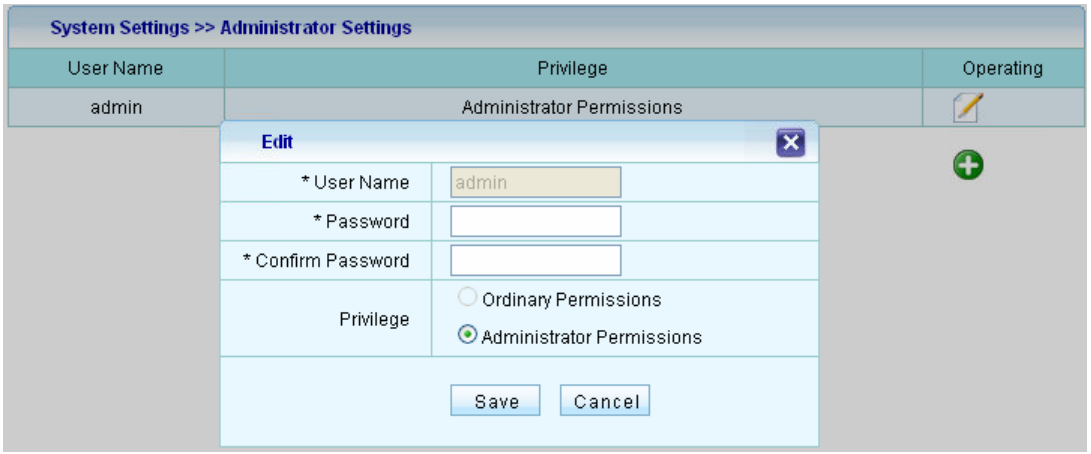


System Settings > Administrator

Item	Description
Username	Enter account username.
Password	Enter password.
Confirm password	Enter password again to confirm.
Privilege	Enter level of account system privilege: • Ordinary • Administrator
Save	Click **Save** to save the values and update the screen.
Cancel	Click **Cancel** to leave the menu without changing current values.

Use these settings to change an account password.

To view the Administrator menu, navigate to System Settings > Administrator.



System Settings > Administrator

Item	Description
Password	Enter new password.
Confirm password	Enter new password again to confirm.
Privilege	Enter level of account system privilege: • Ordinary • Administrator
Save	Click **Save** to save the values and update the screen.
Cancel	Click **Cancel** to leave the menu without changing current values.

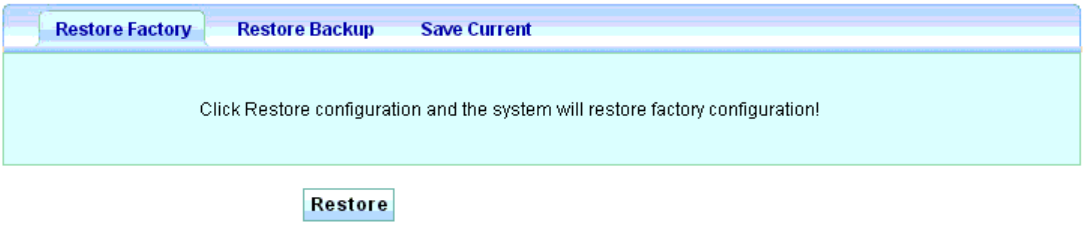
4.10. System Config

Use these settings to restore the device to factory defaults, restore settings from a backup, and save current settings to a backup.

4.10.1. System Config

Restore Factory

To view the Restore Factory menu, navigate to System Config > Restore Factory.

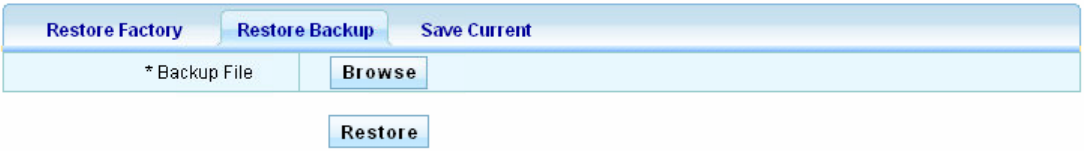


System Config > Restore Factory

Item	Description
Restore	Restore switch to factory default settings.

Restore Backup

To view the Restore Backup menu, navigate to System Config > Restore Backup.

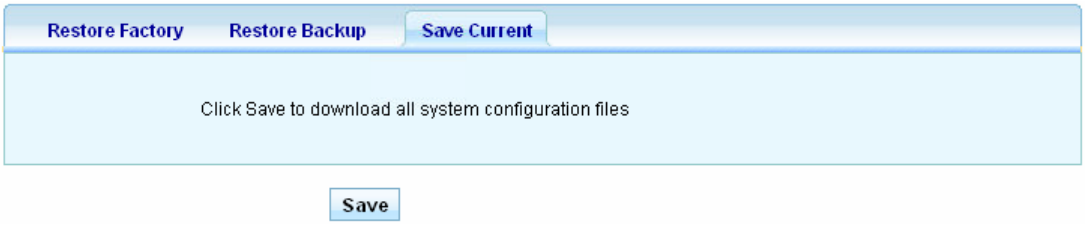


System Config > Restore Backup

Item	Description
Browse	Browse local computer to locate a backup file.
Restore	Restore switch settings from selected backup file.

Save Current

To view the Save Current menu, navigate to System Config > Save Current.



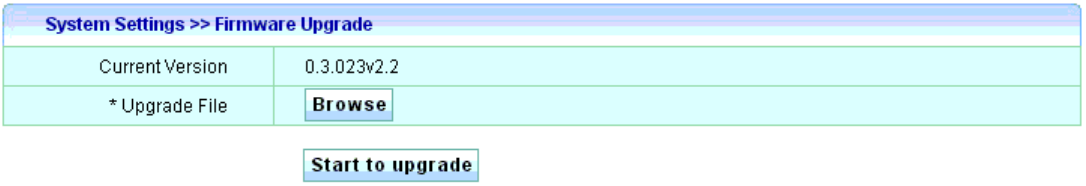
System Config > Save Current

Item	Description
Save	Save current switch settings as a backup file.

4.10.2. Firmware Upgrade

This page allow you to upgrade to new firmware file from a remote TFTP server or from local storage.

To view the Firmware Upgrade menu, navigate to System Config > Firmware Upgrade.



System Config > Firmware Upgrade

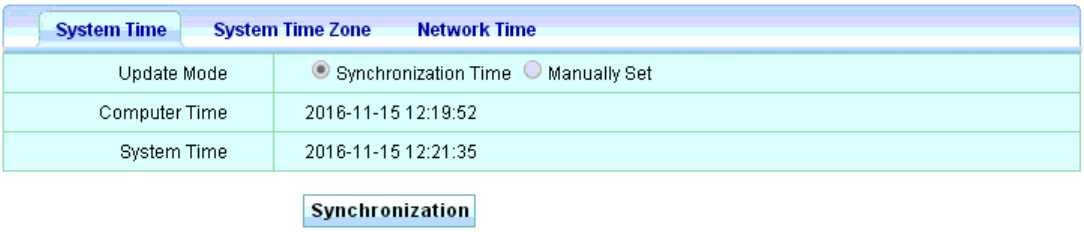
Item	Description
Current Version	Displays currently installed firmware version number.
Browse	Browse local computer to locate a firmware file.
Start to upgrade	Install selected firmware file.

4.10.3. System Time

Use this section to set time zone and time services such as automatic daylight saving synchronization.

System Time

To view the System Time menu, navigate to System Config > System Time > System Time.



System Config > System Time > System Time

Item	Description
Update Mode	Select a method of updating the system time: • Synchronization Time: update system time by synchronizing with a remote source • Manually Set: enter the system time manually
Synchronization	Click to synchronize the system time with a remote source.

System Time Zone

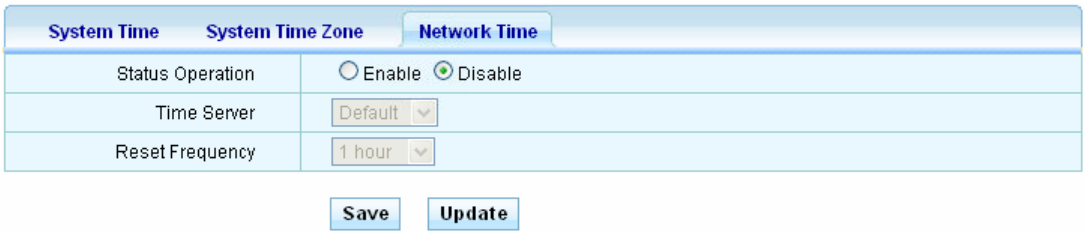
To view the System Time menu, navigate to System Config > System Time > System Time Zone.

System Config > System Time > System Time Zone

Item	Description
Time Zone	Select a global time zone.
Save	Click **Save** to save the values and update the screen.

Network Time

To view the Network Time menu, navigate to System Config> System Time > Network Time.



System Config > System Time > Network Time

Item	Description
Status Operation	Enable/disable network time
Time Server	Online Network Time Protocol (NTP) server queried for accurate time information.
Reset Frequency	Frequency with which the network time is reset.
Save	Click **Save** to save the values and update the screen.
Update	Update system time by synchronizing with online Network Time Protocol (NTP) server.

4.10.4. Reboot

Use this section to reboot the switch, either immediately or after a specific time period.

Reboot Now

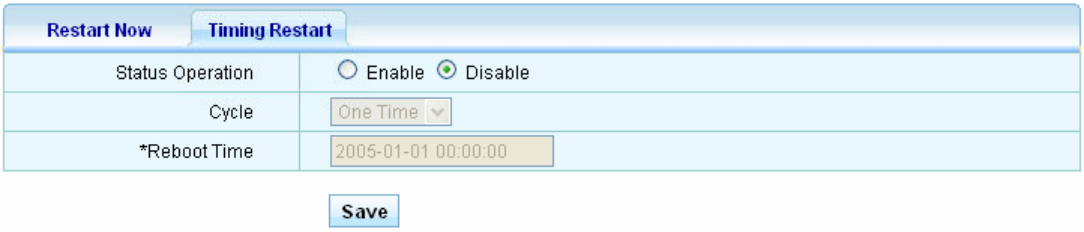
To view the Reboot Now menu, navigate to System Config> Reboot > Reboot Now.

System Config > Reboot > Reboot Now

Item	Description
Reboot	Click to reboot the switch.

Timing Restart

To view the Timing Restart menu, navigate to System Config> Reboot > Timing Restart.



System Config > Reboot > Timing Restart

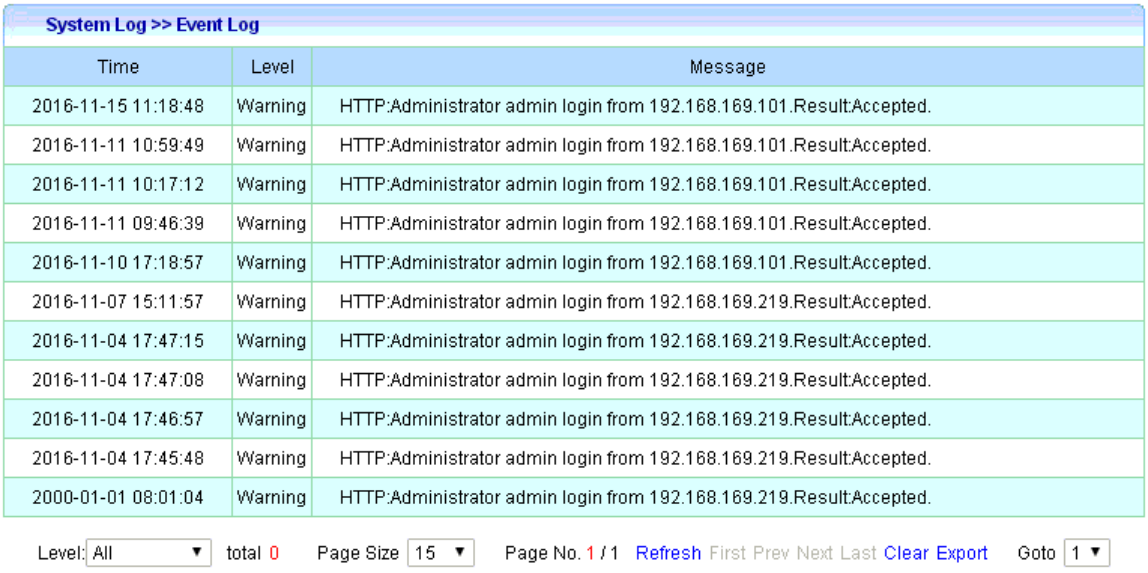
Item	Description
Status Operation	Enable/disable timing restart.
Cycle	Enter the number of times the reboot schedule should execute.
Reboot Time	Enter the time at which the switch should reboot.
Save	Click **Save** to save the values and update the screen.

4.11. System Log

System logs record network events for review and analysis. Download logs as readable files using the **Export** option at the bottom right of each window.

4.11.1. Event Log

To view the Event Log menu, navigate to System Log > Event Log.

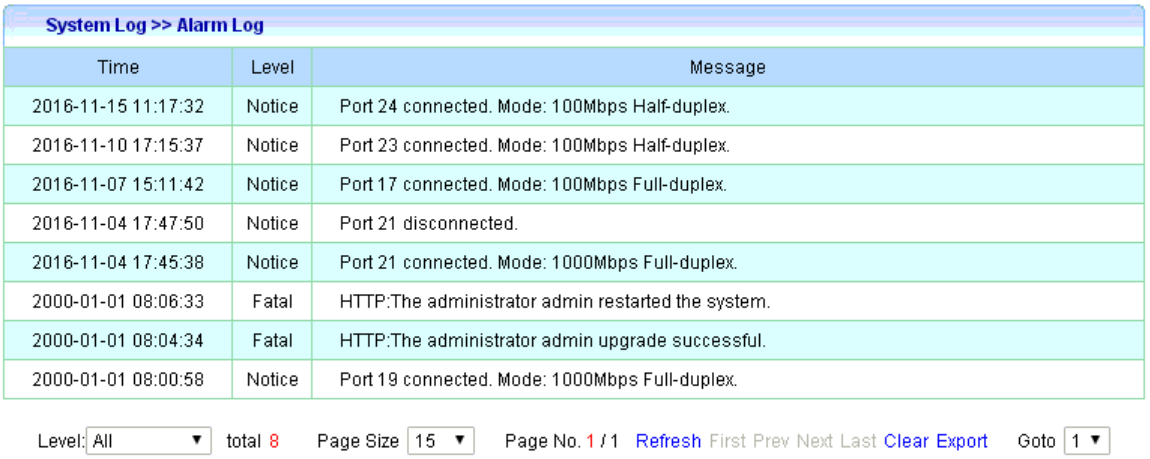


System Log > Event Log

Item	Description
Refresh	Refresh the log to display the latest data.
Clear	Clear all log data.
Export	Download log data as a readable file.

4.11.2. Alarm Log

To view the Alarm Log menu, navigate to System Log > Alarm Log.

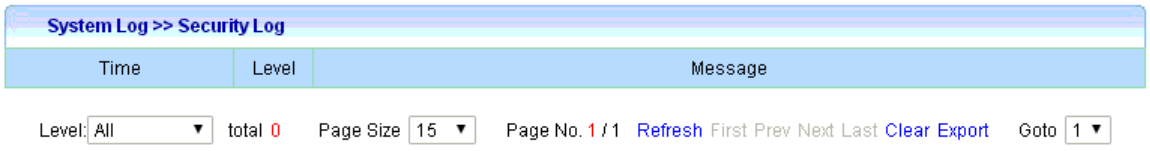


System Log > Alarm Log

Item	Description
Refresh	Refresh the log to display the latest data.
Clear	Clear all log data.
Export	Download log data as a readable file.

4.11.3. Security Log

To view the System Log menu, navigate to System Log > Security Log.



System Log > Security Log

Item	Description
Refresh	Refresh the log to display the latest data.
Clear	Clear all log data.
Export	Download log data as a readable file.

4.11.4. Network Log

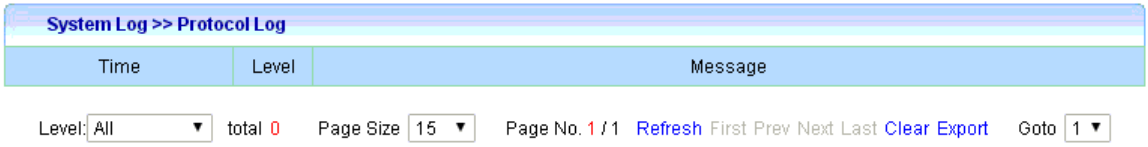
To view the Network Log menu, navigate to System Log > Network Log.

System Log > Network Log

Item	Description
Refresh	Refresh the log to display the latest data.
Clear	Clear all log data.
Export	Download log data as a readable file.

4.11.5. Protocol Log

To view the Protocol Log menu, navigate to System Log > Protocol Log.



System Log > Protocol Log

Item	Description
Refresh	Refresh the log to display the latest data.
Clear	Clear all log data.
Export	Download log data as a readable file.

5. Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

FCC Caution

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE). The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Bulgaria, Cyprus, Czech, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Turkey, and United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not Intended for Use

None

Protect Our Environment

When the equipment has reached the end of its useful life, it must be taken to a recycling center and processed separate from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this switch can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste; you may be subject to penalties or sanctions under the law.